

Patent Assignment Abstract of Title

Total Assignments: 1**Application #:** 10616124**Filing Dt:** 07/08/2003**Patent #:** NONE**Issue Dt:****PCT #:** NONE**Publication #:** US20050010483**Pub Dt:** 01/13/2005**Inventor:** Marvin T. Ling**Title:** Methods and apparatus for transacting electronic commerce using account hierarchy and locking of accounts**Assignment: 1****Reel/Frame:** 015590 / 0079 **Received:** 07/26/2004 **Recorded:** 07/22/2004 **Mailed:** 01/24/2005 **Pages:** 3**Conveyance:** ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).**Assignor:** LING, MARVIN T.**Exec Dt:** 07/16/2004**Assignee:** PAYBYCLICK CORPORATION

15333 NORTH PIMA RD.

SUITE 105

SCOTTSDALE, ARIZONA 85260

Correspondent: LUCE, FORWARD, HAMILTON & SCRIPPS LLP


NICOLA A. PISANO

11988 EL CAMINO REAL, SUITE 200

SAN DIEGO, CA 92130

Search Results as of: 12/6/2005 8:39:09 A.M.

If you have any comments or questions concerning the data displayed, contact OPR / Assignments at 571-272-3350
Web interface last modified: September 28, 2005

- ☐ **15. A mechanism for establishing policies for electronic commerce**
Minsky, N.H.; Ungureanu, V.;
Distributed Computing Systems, 1998. Proceedings. 18th International Conference on
26-29 May 1998 Page(s):322 - 331
Digital Object Identifier 10.1109/ICDCS.1998.679732
[AbstractPlus](#) | Full Text: [PDF\(248 KB\)](#) IEEE CNF
- ☐ **16. Untraceable off-line electronic cash flow in e-commerce**
Wang, H.; Zhang, Y.;
Computer Science Conference, 2001. ACSC 2001. Proceedings. 24th Australasian
29 Jan-4 Feb 2001 Page(s):191 - 198
Digital Object Identifier 10.1109/ACSC.2001.906642
[AbstractPlus](#) | Full Text: [PDF\(652 KB\)](#) IEEE CNF
- 

Day : Tuesday
Date: 12/6/2005
Time: 08:40:27

PALM INTRANET

Inventor Name Search Result

Your Search was:

Last Name = LING

First Name = MARVIN

Application#	Patent#	Status	Date Filed	Title	Inventor Name
09665237	Not Issued	71	09/18/2000	METHOD AND APPARATUS FOR CONDUCTING ELECTRONIC COMMERCE TRANSACTIONS USING ELECTRONIC TOKENS	LING, MARVIN T
09553695	Not Issued	120	04/21/2000	METHOD AND APPARATUS FOR CONDUCTING ELECTRONIC COMMERCE TRANSACTIONS USING ELECTRONIC TOKENS	LING, MARVIN T
09655310	6901170	150	09/05/2000	IMAGE PROCESSING DEVICE AND RECORDING MEDIUM	LING, MARVIN T.
09655314	6873436	150	09/05/2000	IMAGE PROCESSING DEVICE AND RECORDING MEDIUM	LING, MARVIN T.
09717607	Not Issued	94	11/21/2000	METHOD AND APPARATUS FOR AUTOMATIC CLEANING AND ENHANCING OF SCANNED DOCUMENTS	LING, MARVIN T.
09753784	Not Issued	41	01/02/2001	Method and apparatus for conducting electronic commerce transactions using electronic tokens	LING, MARVIN T.
10057420	Not Issued	30	01/25/2002	Systems and methods for conducting electronic commerce transactions requiring micropayment	LING, MARVIN T.
10217859	Not Issued	61	08/12/2002	Systems and methods for distributing on-line content	LING, MARVIN T.
10217871	6876979	150	08/12/2002	ELECTRONIC COMMERCE BRIDGE SYSTEM	LING, MARVIN T.
10434886	Not Issued	41	05/09/2003	Methods and apparatus for anonymously transacting internet shopping and shipping	LING, MARVIN T.
10616124	Not Issued	71	07/08/2003	Methods and apparatus for transacting electronic commerce using account hierarchy and locking of accounts	LING, MARVIN T.
11097889	Not Issued	20	03/30/2005	Method and apparatus for conducting electronic commerce transactions using electronic tokens	LING, MARVIN T.
60177820	Not Issued	159	01/25/2000	Method and apparatus for automatic cleaning and enhancing of scanned	LING, MARVIN T.

				documents	
60178239	Not Issued	159	01/26/2000	Method and System for Placing Orders for Purchasing, Renting or Extending Rental Periods for Computer Software Products or Other Products Using (Or Without Using) a Communication Network	LING, MARVIN T.
60311446	Not Issued	159	08/09/2001	Method and apparatus for conducting electronic commerce for micropayment transactions using electronic tokens or electronic money	LING, MARVIN T.
07277684	Not Issued	161	11/28/1988	AUTOMATIC DRAWING SYSTEM	LING, MARVIN T.
60167330	Not Issued	159	11/24/1999	METHOD AND APPARATUS FOR AUTOMATIC CLEANING AND ENHANCING OF SCANNED DOCUMENTS	LING, MARVIN T.

Inventor Search Completed: No Records to Display.

	Last Name	First Name	
Search Another: Inventor	<input type="text" value="ling"/>	<input type="text" value="marvin"/>	<input type="button" value="Search"/>

To go back use Back button on your browser toolbar.

Back to [PALM](#) | [ASSIGNMENT](#) | [OASIS](#) | [Home page](#)

Refine Search

Search Results -

Terms	Documents
709/204	2825

Database:

US Pre-Grant Publication Full-Text Database
 US Patents Full-Text Database
 US OCR Full-Text Database
 EPO Abstracts Database
 JPO Abstracts Database
 Derwent World Patents Index
 IBM Technical Disclosure Bulletins

Search:

Search History

 DATE: Tuesday, December 06, 2005 [Printable Copy](#) [Create Case](#)

Set Name Query

side by side

Hit Count Set Name

result set

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR

L36	709/204	2825	L36
L35	709/203	10186	L35
L34	709/224	7884	L34
L33	709.clas.	40767	L33
L32	705.clas.	38307	L32
L31	235.clas.	93910	L31
L30	235/380	8396	L30
L29	705/38	923	L29
L28	705/41	718	L28
L27	705/1	5289	L27
L26	5815657.pn.	2	L26
L25	6236981.pn.	2	L25
L24	5839119.pn.	2	L24
L23	5920861.pn.	2	L23
L22	5287269.pn.	2	L22
L21	5963924.pn.	2	L21
L20	6236981.pn.	2	L20

DB=USPT; PLUR=YES; OP=OR

L19 '5872844'.pn. 1 L19

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR

L18 6341273.pn. 2 L18

L17 6449601.pn. 2 L17

L16 6473500.pn. 2 L16

L15 6493683.pn. 2 L15

DB=USPT; PLUR=YES; OP=OR

L14 '6105006'.pn. 1 L14

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR

L13 6473740.pn. 2 L13

L12 l10 and l11 94 L12

L11 705/39 1729 L11

L10 L9 and (secondary or second or sub-account or subaccount) 512 L10

L9 L8 and (first or main or primary) near account 526 L9

L8 L7 and (funds with transfer or funds near transfer or funds adj transfer) 4548 L8

L7 L6 and goods or services 297097 L7

L6 L5 and (user or customer or individual) 622 L6

L5 L4 and (vendors or merchants or suppliers) 625 L5

L4 L3 and (website or web with site or web near site) 901 L4

L3 L2 and (e-shopp\$ or internet with shopp\$) 1516 L3

L2 (e-commerce or "electronic commerce") 22785 L2

L1 705/39 1729 L1

END OF SEARCH HISTORY

[First Hit](#) [Previous Doc](#) [Next Doc](#) [Go to Doc#](#)

Generate Collection

Print

L12: Entry 31 of 94

File: PGPB

Dec 19, 2002

DOCUMENT-IDENTIFIER: US 20020194122 A1

TITLE: Credit extension process using a prepaid card

Classification at Publication, US Primary Class/Subclass:705/39Brief Description of Drawings Paragraph:

[0012] FIG. 2 shows a flow diagram of a process wherein a second financial institution facilitates a credit transaction based upon loan performance at a first financial institution wherein the credit rating for the loans is established by deposit and purchase transactions of a prepaid card customer.

Detail Description Paragraph:

[0018] FIG. 1 shows a block diagram of a system operating in accordance with the present invention. A consumer may make deposits in an account using an automated currency processor 100, such as the automated currency processor described in U.S. patent application Ser. No. 09/939,940 of which is hereby incorporated by reference. The automated currency processor receives deposits 102. The deposits 102 include cash received in the form of paper or coin currency. The deposits 102 further include other electronic transfers such as those facilitated by credit card, prepaid card, smart card and other active or passive card transactions. The deposits from the automated currency processor are processed by a financial processor 150 which attributes the deposits to an account balance 155 associated with the customer. The customer preferably uses a prepaid card 105 to identify the account 155. The prepaid card may be any type of account card identifying account 155 including active smart cards and passive prepaid and credit cards. The consumer may use the prepaid card 105 to purchase goods or services from a consumer point of sale 110. The financial processor receives a transaction request from the consumer point of sale 110 and attributes it to account 155 with information provided by prepaid card 105. Additional transaction verification may be done by entry of a PIN by the customer or signature verification at point of sale 110. If the account balance 155 is sufficient to fund the transaction then the transaction is authorized by transaction authorization 160.

Detail Description Paragraph:

[0019] The aforementioned process allows for a customer to anonymously use a card at a point of sale to complete a transaction. No personal information is required to establish an account at the automated currency processor 100, and no personal information is required at consumer point of sale 110 to complete the transaction. Further, fund transfers into account 155 at the automated currency processor need not identify the customer. For example, funds can be transferred into the customer's account using a credit card of another at the automated currency processor. The credit card need not be the customer's credit card. For example, a prepaid card customer may perform a few hours of repair work and be compensated by the one employing the prepaid card customer. Instead of check or cash compensation, a credit card transfer of funds at the automated currency processor into the customer's account may be made by debiting the employer's credit card. Alternatively the transfer may occur over the Internet with a browser accessing the customer's account. See www.mycardstatus.com for an example an Internet based credit card transfer of funds into the account of a prepaid card.

Detail Description Paragraph:

[0026] The credit processor analyzes the transaction classification 178. Transaction classification indicates the types of goods or services being purchased. Since the consumer could be anonymous, the extension of credit may only be made for certain types of goods or services. For example automotive repair services may merit extension of credit, while credit may not be extended for services at a casino. Further, credit may be extended for a class of

goods or services regularly purchased by the consumer. For example, if the consumer has a history of purchasing nursing services, then credit could be extended for the continued purchase of nursing services, even though purchased at a new point of sale.

Detail Description Paragraph:

[0034] FIG. 2 shows a flow diagram of a process wherein a second financial institution facilitates a credit transaction based upon loan performance at a first financial institution wherein the credit rating for the loans is established by deposit and purchase transactions of a prepaid card customer. In step 50, deposits are received. The deposits are preferably non-anonymous or alternatively anonymous depending on whether or not the customer associated with the account has provided personal information identifying the customer. The deposit may be a cash deposit at the automated currency processor, or other electronic fund transfer. Then in step 52 any loan granted (from step 66) is repaid (either settled or paid down depending upon the amount deposited, the minimum payment and/or directions from the customer) from the deposit and the remaining funds transferred into a first account. The first account is preferably a prepaid card account established by the customer. Then in step 56 a credit limit is determined based upon the account deposit, purchase and loan transactions. Preferably, the credit limit is determined only if the customer has provided personal information identifying the customer. The personal information includes name and address information but preferably does not include other financially related information such as bank account, loan and credit status or property ownership information. In another embodiment, if the customer's prepaid card account was initially established as anonymous and then personal information provided some time thereafter, the anonymous deposits and purchases can be used in determining the first credit limit upon validation. Several methods of validation are described below. In yet another embodiment the customer's credit limit may be established even if the customer is anonymous, as described in more detail below. Then in step 58, a purchase transaction request is received. The request may be either anonymous or non-anonymous depending upon whether the customer as provided personal information. Step 60 determines if the first account has sufficient funds. If so, then the transaction is authorized in step 62 thereby facilitating the purchase. If there are not sufficient funds then step 64 determines if the credit limit is sufficient to cover the transaction. If not, no authorization is generated. If so, then a loan is granted at step 66 equivalent to the amount beyond the account balance needed to facilitate the transaction and the transaction authorized at step 68. The granting of the loan may invoke additional charges such as loan origination and interest fees. The loan granting at step 66 and loan repayment of step 52 are useful in the establishing of credit beyond the first credit limit determined by the prepaid card company hosting the first account. Step 70 generates non-anonymous credit information from the loan information for use by other financial institutions for extension of credit to the customer. This credit information is non-anonymous when identification of personal information related to the customer is required by the other financial institutions in the extension of credit. Since the extension of credit at step 56 may have occurred while the customer was anonymous, the loan granting and repayments may be further validated as described below. Steps 72-74 are preferably performed by a separate financial institution or credit agency. Step 72 determines a second credit limit for a second account based in part on the loan granting and repayments of the first account at steps 66 and 52. Other conventional credit information may be processed such as bank assets and other credit performance and other tangible or intangible assets and incomes. In step 74 a purchase request for the second account is received. If there is sufficient credit limit then the transaction is authorized at step 76.

Detail Description Paragraph:

[0035] FIG. 2 show a process wherein a customer may anonymously open a first account using cash deposits at an automated currency processor and use a prepaid card to facilitate anonymous purchases. A prepaid card credit limit is established based upon a history of deposit, purchase and loan transactions facilitated by the financial processor. No other credit information is required. This has the advantage of providing credit to customers who may be unworthy of credit by conventional standards by utilizing a history of prepaid card transactions that would have otherwise been facilitated with cash. When the customer uses the prepaid card credit, loan granting and loan repayment by subsequent deposits results. The loans and loan repayment history is useful and is used by another financial institution to extend other types credit to the customer for other purchasers. The customer provides personal information prior to the extension of credit by the second financial institution, thereby making all subsequent deposit, purchase and loan transactions non-anonymous. The process has the further advantage of validation steps which allow use of the prior anonymous transactions in the determination of credit limits. Thus, the transaction history developed while the customer was anonymous remains

applicable.

Detail Description Paragraph:

[0037] For example, if a customer makes weekly deposits of \$500 for twenty six weeks, then a credit of \$300 is available for the prepaid card customer. Prior to the completion of the 26 weeks it is anticipated that the customer is purchasing goods or services at points of sale at a rate substantially equal to the deposit rate. Thus, a typical prepaid card customer depositing \$500 a week is also spending about \$500 a week with the prepaid card. After credit is advanced between weeks 26 and 51, the minimum weekly payment is 25% of the loan granted. Thus, if a customer receives a \$300 loan, the next minimum weekly deposit is \$75. If this deposit is not made then a missed loan payment may be reported to other institutions. If this deposit is made then a satisfactory loan payment may be reported to other institutions. In order to advance to the next credit level, the next total deposit after the \$300 loan must be at least \$575, equal to the weekly deposit of \$500 plus the minimum weekly payment of \$75. The customer may direct that the deposit includes more than the minimum weekly payment of credit. For example, if the customer's weekly deposit were \$650 instead of \$575 then the customer could direct that \$100 be applied to loan repayment (rather than the \$75 minimum) and the remaining \$550 be deposited in the account. This example works not only to accelerate loan repayment but accelerates the customer's building of credit available with the prepaid card. The customer's direction may be made at the time of deposit, via instructions over the internet or at other times or means as are known by those familiar with the art. If this the loan is entirely repaid then both the periodic loan payments and a satisfactory loan repayment may be reported to other institutions. If the customer continues to deposit \$500 per week plus additional minimum weekly payment, then after 52 weeks the available credit is increased to \$600 per month and the minimum weekly payment after credit is advanced is decreased to 10% of the credit advanced. This reflects the customer's improved creditworthiness. If the minimum weekly payment is not met, then a missed payment may be included in credit information provided to other financial institutions.

Detail Description Paragraph:

[0040] FIG. 3 shows a flow diagram of a process for establishing credit after provision of personal information in accordance with the present invention. Steps 200 through 212 show the transaction method when the customer is anonymous and no credit is extended while steps 214 through 224 show the transactions when the customer is no longer anonymous and credit may be extended. Note that in alternate embodiments credit can be extended while the customer remains anonymous. Step 200 receives anonymous cash and other deposits at a currency processor wherein information associated with the prepaid card identifies the account. For example, referring to table 1 above, the customer may be anonymous for the first 12 weeks and then provide personal information, making additional deposits thereafter. The initial 12 weeks of deposits may be considered in determination of credit. It should be appreciated that for non-cash transfers of step 200, that alternative devices and methods other than a currency processor may be used to facilitate the transfer. Such alternatives include conventional wire transfers and Internet based transactions. Step 204 receives a transaction authorization request from a point of sale wherein the prepaid card identifies the account. Step 206 determines if sufficient funds are available to cover the transaction. If so the transaction is authorized in step 208. Alternately, if there are insufficient funds then the transaction is not authorized in step 210. Corresponding account debiting and funds transfer to the point of sale merchant are not shown. Step 212 checks if personal information is associated with the account. The personal information includes customer credit information. If not, the process returns to step 200 and/or 204 to await for another deposit or purchase transaction. If personal information is received, then step 214 receives non-anonymous deposits. Deposits may be received with information indicative of the account included on the prepaid card, or may be received with information indicative of the customer as included in the personal and credit information provided at step 212. Then, step 216 determines a credit limit based upon anonymous and non-anonymous purchases and deposits, and personal information including credit information. Step 218 receives a transaction authorization request from a point of sale. Step 220 determines if the sum of the credit limit and the account balance is sufficient to cover the transaction. Step 222 grants the loan and authorizes the transaction if the sum is sufficient, otherwise the transaction is not authorized at step 224. Corresponding account debiting and funds transfer to the point of sale merchant are not shown. It should be appreciated that the amount of credit may be modified based upon the classification of the point of sale requesting authorization or the classification of goods and/or services associated with the transaction request at step 218. Thereafter the process returns to steps 214 through 218 to receive deposits, transaction authorization requests and determine credit limits.

Detail Description Paragraph:

[0041] FIG. 4 shows a flow diagram of a process for extending credit on the basis of account transactions in accordance with the present invention. Payroll deposits are received at step 240, such deposits are optional. In step 242, cash and other deposits are received. Information included with the prepaid card associates cash and other deposits with the account. If the account is not anonymous, then personal and credit information may be used to direct the deposit to the account. A transaction authorization request is received from a point of sale at step 244 wherein the prepaid card is used to identify the account. The transaction is authorized if the account has sufficient funds, steps 246 and 248. If insufficient funds, steps 250 through 260 determine if credit should be extended. Step 250 determines if there is an acceptable deposit history to cover the insufficiency. For example credit may be extended up to the value of the next anticipated deposit. As a modification or alternative to the example of Table 1 above, a statistical example of determining how much credit to extend includes; extending no credit if deposits have not been regular for six months, extending credit equal to 10% of the next expected deposit upon the six month, linearly increasing to 50% of the next anticipated deposit through the twenty fourth month, and maintaining the credit limit to 50% of the next anticipated deposit thereafter. If the deposit is a payroll deposit, step 252 may further verify employment with the employer to assure the employee is still an employee and/or to ensure the viability of the employer. Such employment and employee checks may be automated. The credit is preferably adjusted to reflect the statistical risk of receiving the employer payroll deposit. Step 254 determines if the point of sale is acceptable. This step additionally determines credit based upon the aforementioned classification associated with the point of sale. For example, if the point of sale is a liquor store, then credit may be denied or reduced by a factor associated with the classification. Step 256 determines if the goods and/or services to be purchased are acceptable. This step additionally determines credit based upon the aforementioned classification associated with the goods and/or services being purchased. For example, if purchasing services in a casino is attempted, then credit beyond the amount deposited in the account may be denied or reduced by a factor associated with the classification. It should be appreciated that weekly deposits of Table 1 may be enhanced or substituted with weekly purchase information. This has the additional advantage of being able to determine a credit limit further in response to an assign a credit quality factor associated with the points of sale used by the prepaid card customer. Step 258 determines if the personal and/or credit information related to the account is acceptable. This applies to more conventional credit establishment processes based on customer supplied information and/or information provided by financial institutions and credit providers. This step may substantially modify the amount of credit determined by the prior steps. For example, if the customer is anonymous then the credit extended may be reduced. However, if it is known that the customer has substantial assets and/or deposits at a bank or other financial institution, then credit may be greatly increased. If the extended credit of step 260 plus the account balance is sufficient to cover the transaction, then it is authorized at step 248 and a loan granted. Otherwise the transaction is not authorized at step 262.

Detail Description Paragraph:

[0043] FIG. 5 shows a flow diagram of a process for validating anonymous deposits and purchases prior to provision of personal and credit information for the purpose of credit determination. In this embodiment, anonymous transactions are allowed and tracked, but credit is not extended until after personal and/or other credit information is provided. Anonymous deposits are received at step 300. The location and source characteristics of the deposit are determined at step 302. If cash is deposited at a currency processor, then the location of the currency processor and the amount of the deposit is determined. If another fund transfer method is used, then the source and amount of deposit is determined. In step 304, a transaction is authorized. Step 306 determines the location and other characteristics of the point of sale. The location of the point of sale and deposit location information help to establish a customer's neighborhood. The determination of other characteristics allows determination of the types of stores a consumer shops. Step 308 determines characteristics of goods and services purchased. The aforementioned steps are repeated for all deposits and purchases and help to establish a profile for the anonymous customer. In step 310 the personal and credit information is received from the customer. Step 312 receives deposits and authorizes purchase transactions, albeit with a now non-anonymous customer. Step 314 establishes a profile of the non-anonymous customer by determining the location and source characteristics of non-anonymous deposits and location and other characteristics of points of sale and characteristics of good and/or services purchases. Step 316 allows inclusion of the anonymous deposits of step 300 and anonymous purchases of step 304 at step 318 if the anonymous and non-anonymous characteristics or customer profiles

substantially match. Matching profiles include substantially similar profiles that exclude a substantial portion of the population by use of the profiles, thereby reducing the likelihood of theft or fraud. It should be appreciated that step 316 could be modified to weigh the anonymous purchases and deposits on the basis of the similarity between the anonymous and non-anonymous customer profiles. Matching profiles would provide the most weight, while similar profiles, where for example the customer is purchasing goods or services of a slightly different characteristic would reduce the weighing of the anonymous purchases and deposits. Profiles that are completely different may be indicative of theft or fraud and result in no weighing of anonymous purchases and deposits as well as no credit based upon non-anonymous purchases and deposits.

Detail Description Paragraph:

[0045] FIG. 6 shows an alternate process for credit extension and transaction validation based on the BIO-ID of the customer. While the process of FIG. 5 in part protects the credit provider from extension of credit due to fraud by validating the anonymous and non-anonymous customer profiles to assure a customer's continuity. The process of FIG. 6 in part protects the credit provider from extension of credit due to fraud or theft by validating the BIO-ID or other biometric indicia of the customer. This is an alternative for or supplement to profile comparisons or other processes for validating anonymous deposits and transactions and has the advantage of not requiring additional personal and/or credit information in the extension of credit. The customer can be positively identified from one transaction to the next as being the same customer, without necessarily knowing the identity of the customer because of a matching BIO-ID. Step 350 receives anonymous deposits, repays loans and authorizes anonymous transactions while processing the associated BIO-IDs. When a customer makes a deposit or a purchase at a consumer point of sale, the BIO-ID is determined by finger print, retinal scan or otherwise thereby validating the customer. Step 352 determines the location and source characteristics of deposits, the location and other characteristics of the point of sale and characteristics of goods and/or services being purchased. Step 354 determines if there is a substantial match identifying the customer between anonymous BIO-IDs of the current transaction with prior purchases and deposits. If no match, the transaction is not authorized at step 358. If there is a match, then step 358 determines a credit limit based on anonymous deposits and purchases. If there are sufficient funds in the account plus the determined credit limit to cover the transaction in step 360 then a loan is granted and the transaction is authorized in step 362. Thus, credit has been extended to a customer who is anonymous yet positively identified as a prior customer.

CLAIMS:

1. An automated method of authorizing a consumer purchase comprising the steps of: receiving a first deposit transaction depositing funds within a first account; determining a first credit limit associated with the first account wherein the first credit limit is based upon account information associated with the first account; receiving a request for authorization of a purchase transaction associated with the first account; authorizing the purchase transaction if funds within the first account plus the first credit limit are to sufficient to facilitate the purchase transaction; determining a loan amount in response to an amount of the first credit limit utilized for said step of authorizing; granting a loan in response to the loan amount; receiving a subsequent deposit transaction having additional funds associated with the first account; applying a loan repayment portion of the additional funds to at least partial repayment of the loan and transferring a remaining portion of the additional funds to the first account; and generating credit information indicative of the loan granting and loan repayment.
2. The method of claim 1 wherein the account information consists substantially only of deposit transaction information, purchase transaction information, any loan granting and repayment information, and any provided personal information indicative of a person associated with the first account but does not include other financial information related to the person.
3. The method of claim 1 wherein the account information consists substantially only of deposit transaction information and personal information indicative of a person associated with the first account but does not include other financial information related to the person.
6. The method according to claim 1 wherein the loan repayment portion of the additional funds is an amount greater than a predetermined minimum amount wherein the loan repayment porting is indicated by a person associated with the first account.

7. The method according to claim 1 further comprising the steps of: determining a second credit limit amount associated with a second account substantially independent of the first account in response to the credit information; receiving a request for authorization of a second purchase transaction associated with the second account; and authorizing the second purchase transaction if the second credit limit amount is sufficient to facilitate the second purchase transaction.

8. The method according to claim 1 wherein the preceding steps are performed by a first financial institution and the subsequent steps are performed by a second financial institution substantially independent of the first financial institution, the method at the second financial institution comprising the steps of: determining a second credit limit amount associated with a second account substantially independent of the first account in response to the credit information received from the first financial institution; receiving a request for authorization of a second purchase transaction associated with the second account; and authorizing the second purchase transaction if the second credit limit amount is sufficient to facilitate the second purchase transaction.

9. The method according to claim 1 further comprising the steps of: receiving a plurality of deposit transactions depositing funds into the first account; authorizing each of a plurality of purchase transactions if funds within the first account are sufficient to facilitate each of the plurality of purchase transactions; and including the plurality of deposit transactions and purchase transactions in the account information; wherein said step of determining the first credit limit determines the first credit limit to be substantially zero upon reception of the first deposit transaction and increases the limit in response to the account information of said step of including.

10. The method according to claim 9 wherein at least a portion of the transactions of said steps of receiving the plurality of deposit transactions and authorizing the plurality of purchase transactions are anonymous, without identification of a person associated with the first account, and the method further comprises the step of: receiving personal information identifying the person associated with the first account wherein said step of determining the first credit limit includes account information from the plurality of anonymous deposit and purchase transactions in the determination of the first credit limit.

11. The method according to claim 10 wherein the anonymous deposit transactions include cash deposits received at an automated currency processor using a card having information identifying the first account but not the person, and the anonymous purchase transactions are facilitated by the card having the information identifying the first account but not the person.

13. The method according to claim 12 further comprising the steps of validating that the anonymous deposit and purchase transactions were caused by the person associated with the first account, wherein said step of determining the first credit limit is further responsive to said step of validating.

16. The method according to claim 1 wherein at least a portion of the loan granting and repayment are anonymous, without identification of a person associated with the first account, and the method further comprises the step of receiving personal information identifying a person associated with the first account wherein said step of generating credit information includes anonymous loan and loan repayment information occurring prior to said step receiving personal information.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#) [Previous Doc](#) [Next Doc](#) [Go to Doc#](#)

Generate Collection

Print

L12: Entry 29 of 94

File: PGPB

Jan 9, 2003

DOCUMENT-IDENTIFIER: US 20030009420 A1
TITLE: Automated payment system and method

Abstract Paragraph:

An automated payment system for processing payment by a customer to a company. The payment system includes a document scanning system which has an input receptacle adapted to accept a document. After receiving an authorization agreement from the customer, the scanner acquires at least one image from the document. Also provided is a first computer adapted to receive images from the document scanning system. Adapted to communicate information represented by the image, a first communication link couples the document scanning system and the first computer. The payment system also includes a second computer adapted to receive images which is in communication with the first computer via a second communication link. The second communication link is adapted to communicate images and payment information.

Classification at Publication, US Primary Class/Subclass:
705/39

Summary of Invention Paragraph:

[0002] Some banks provide invoice payment services for customers who travel frequently. The bills are forwarded directly to the bank, and an employee of the bank writes the check or debits the customer's account for the payment. Because the customer's bank may not be the bank of the company, however, the bills still need to be mailed to the lock box for processing.

Summary of Invention Paragraph:

[0003] Another method recently instituted by some banks and companies is payment via the internet. Such systems vary, but there are two main methods. In one method, a customer enters the company's website and selects a payment option. The customer may then enter important data such as name, address, e-mail address, and the account number they wish to have credited. Also, the customer must provide authorization for the transaction to occur and supply information regarding from where the payment should be debited, i.e., bank name and routing number and account name and number. After the program is established, the user may pay bills on-line. This method takes time (up to three or four days), however, because the company must first send a request to the customer's bank and then wait for the bank to send the funds and for the receiving bank to process the transfer of funds.

Summary of Invention Paragraph:

[0004] The other method of paying on-line is utilized by the customer accessing his or her bank account and sending the information that way. In this system, the bank of the customer processes the transaction on-line and electronically transfers the funds to the company. This process is usually faster because the customer's bank is immediately sending the funds instead of waiting for a request from the company. This method also, however, has drawbacks. First, not all people have access to the internet. Although many people have computers, large segments of the population do not or do not know how to use the internet. Second, due to security issues, not all people who have access to the internet feel comfortable accessing accounts on-line. Some people do not want to provide account numbers on the internet for fear of hackers obtaining such information.

Summary of Invention Paragraph:

[0008] According to one embodiment of the present invention, an automated payment system for processing payment by a customer to a company is provided. The payment system includes a document scanning system, which has an input receptacle adapted to accept a document. After receiving an authorization agreement from the customer, the scanner acquires at least one image from the document. Also provided is a first computer adapted to receive images from the

document scanning system. Adapted to communicate information represented by the image, a first communication link couples the document scanning system and the first computer. The payment system also includes a second computer adapted to receive images which is in communication with the first computer via a second communication link. The second communication link is adapted to communicate images and payment information.

Detail Description Paragraph:

[0031] Customers write out and mail numerous checks in a month. These checks are written to payees for any number of reasons. The check may be to a company to pay a bill or invoice, or it may be written to a person as a gift. The term "customers" refers to any person or business that receives invoices requesting payment from anyone, a person or an entity. The term "payee" refers to whom the money is owed or to whom it is being paid. The term "payee," as used in this application, refers to any person or business who provides services and/or goods to a customer or to anyone to whom a customer wishes to pay money (i.e., a grandchild for a birthday present). The payee may send an invoice to the customer for payment. The term "invoice" refers to any sort of bill, payment coupon, remittance, or reminder notice of payment due for goods or services rendered. As described above in the background, this method of paying invoices often takes a great amount of time and is inefficient. In one embodiment of the present invention, the invoices or bills are mailed directly to a payment center for processing. The term "payment center" includes banks, savings and loans, investment houses, and all other types of financial institutions, whether private, public, or government, as well as including any other business that would provide this service, such as a currency exchange, department or other retail store, or places that normally accept bill payments. For ease of description, the following embodiments will be described in terms of banks, but it is understood that all other payment centers are contemplated.

Detail Description Paragraph:

[0035] The first computer 130 of the payor bank is then linked via a second communication link 140, which is defined the same as above, to a second computer 150 at a payee bank. The payee bank is a bank having an account owned by the payee. The second communication link 140 allows the payor bank to communicate with the payee bank. In this embodiment, images obtained from the scanning system 110 may be transferred to the first computer 130 for debiting the customer's account and then transferred to the second computer 150 for crediting the payee's account. The images are transferred over the communication lines 120, 140. These transfers may occur substantially immediately. For example, an image that is scanned on a Monday morning may be electronically transferred to the receiving bank that day for crediting to the company's account within minutes. Alternatively, the transaction may occur within a couple of hours, depending on the speed of transmission and auditing requirements. In other embodiments, the payee and payor banks may have predetermined time periods established for the transfer of images. For example, the payor bank may send image transmissions once every hour, once a shift, or once a certain number of images have been obtained.

Detail Description Paragraph:

[0037] In other embodiments, the third computer is operated by the customer and a fourth computer operated by the payee is included. Also, the third and fourth computers 170 may be linked to the second computer 150 instead of or in addition to the first computer 130. In all of these embodiments, the operation of the system is the same.

Detail Description Paragraph:

[0048] One example of the arrangement of an image scanner 550 for use in the above-mentioned embodiments is described with reference to FIG. 5. A document 505 having two sides, for example, a check, U.S. or foreign currency, or an invoice, is inserted into the document scanning system 310 (shown in FIG. 3) at position 500a. In the embodiment of FIG. 4, the image scanner 450 is adapted to scan both sides of the document 505. Often, the document 505 contains valuable information on both sides and, thus, obtaining an image of both sides is useful. For example, if the document 505 is a check, a first (or front) side of the check may contain payee and amount information, while a second (or back) side may contain endorsement information.

Detail Description Paragraph:

[0049] After the document 505 is inserted into the document scanning system 310, the document 505 is transported past a scanning arrangement by the transport mechanism 440 (FIG. 4). When the document 505 moves into a position 500b, it is illuminated by a light 560, causing the image of the first or second sides of the document to travel along a first path 510 to a mirror 520. The image is then reflected by the mirror 520 along a second path 530 to a scan head 540,

where the image is obtained. The scan head 540 may be rotatable as shown. The light 560 may be located in various places in the image scanner 450. Thus, one side of the document 505 is imaged using reflection techniques. The document 505 then moves into position 500c where the image of the other of the first and second sides of the document 505 is scanned by the scan head 540 via a path 570. In one embodiment, the transport mechanism 440 stops at the position 500b while, in other embodiments, the transport mechanism 440 operates in continuous motion and does not stop at the various positions for imaging.

Detail Description Paragraph:

[0061] Turning now to FIGS. 9 and 10, an image file of a check and an image file of an invoice are described. Turning first to FIG. 9, a check image file 900 comprises several parts. A first image section 905 represents one side of a scanned check. The image is a collection of encoded data and is represented here pictorially so as to be readily understandable to those skilled in the art. In the check sample shown in FIG. 9, both sides of the check have been scanned. In other embodiments, it may only be desired to scan one side. In the embodiment illustrated, the first image section 905 is the front side of the scanned check. Similarly, a second image section 910 comprises data representing the reverse side of the document, in this case, the back side of the check. Area 915a is the MICR data scanned and is extracted from the full image scan and inserted into a MICR field 915b. The MICR information on the check includes the bank routing number (or ABA number), the payor's checking account number, check number, and may include the dollar amount of the check.

Detail Description Paragraph:

[0069] In both the image files 900 and 1000, there is certain information that should be the same. For example, a customer wanting to pay an invoice from Credit Services should have a check that names Credit Services as the payee. Also, the transaction amount field 960b of the check (FIG. 9) should match the amount field 1030b on the image file 1000 of the invoice. As discussed above, in one embodiment, the document scanning system 310 includes control panels 320, 330 (FIG. 3). The control panels 320, 330 may be used to view the image files 900 and 1000 to insure that the certain fields match. This would alleviate accounting problems for both the customer and the payee in reconciling the customer's account with the payee.

Detail Description Paragraph:

[0086] The document scanning system 1210, via the link with the office computer 1275, may process transactions substantially immediately. That is, withdrawals may be processed in real time rather than waiting for the end of the day. Alternatively, the document scanning system 1210 may transfer the funds at set periods during the day. For example, the funds and images could be transferred once an hour or once a shift. Alternatively, the office computer 1275 could direct the controller when to transfer the images.

Detail Description Paragraph:

[0092] FIGS. 15 and 16 depict an exterior perspective view and a side cross-sectional view of a compact multi-pocket document scanning system 6010. The process for carrying documents through the system is the same as discussed above, except that the processing system has two output receptacles 6217a, 6217b. In this embodiment, a diverter 6260 directs the documents to either the first or second output receptacle 6217a, 6217b. When the diverter 6260 is in a lower position, documents are directed to the first output receptacle 6217a. When the diverter 6260 is in an upper position, documents proceed in the direction of the second output receptacle 6217b.

Detail Description Paragraph:

[0094] FIG. 17 depicts a flow chart for another embodiment of the present invention. In this embodiment, the customer receives the invoice directly and may bring it to the bank or a location having the scanner to pay the bill. In step 1700, the customer brings the payment coupon or invoice to the bank. For demonstration purposes only, a bank will be used as the place of payment. It is also understood, however, that the place of payment may be anywhere with a scanning system of the present invention. For example, it is contemplated that currency exchanges may have document scanning systems and charge a fee for the service. Also, it is contemplated that other sites that currently offer customers invoice payment services (such as department stores that have drop boxes for payment of in-house credit cards or other locations that accept payment of utility bills) may offer the document scanning system of the present invention as a new method of payment. It is also contemplated that the document scanning systems may be stand alone machines which operate in the same manner as an Automated Teller Machine (ATM).

Detail Description Paragraph:

[0101] In this embodiment, the scanning system also includes a second input receptacle 1815 adapted to receive invoices. This is useful for situations where a customer is scanning checks and invoices to be paid by the checks. In this system, a second transport mechanism 1825 transports the invoices 1805 past a second image scanner 1845 and to an output receptacle 2035. The second image scanner 1845 is controlled by the controller and directs images to the memory 1860. The memory 1860 operates as described with reference to FIG. 4.

Detail Description Paragraph:

[0102] The second input receptacle 1815 may also be used to accept currency bills. This is useful if a customer wants to deposit funds as well as pay a check. Alternatively, one input receptacle may be for checks written by the customer to pay bills, and the other input receptacle may be for currency bills and checks written to the customer for deposit into the customer's account at the payor bank.

Detail Description Paragraph:

[0104] Turning now to FIG. 19, another embodiment of a scanning system having two input receptacles is illustrated. In this embodiment, an invoice 1900 is inserted into a first input receptacle 1910. A first transport mechanism 1920 transports the invoice 1900 from the first input receptacle to a second transport mechanism 1927. The second transport mechanism 1927 transports the invoice 1900 past an image scanner 1940 and to an output receptacle 1930. A second input receptacle 1915 is also included in the scanning system and is adapted to receive a check 1905. A third transport mechanism 1925 transports the check 1905 from the second input receptacle 1915 to the second transport mechanism 1927. The second transport mechanism 1927 transports the check past the image scanner 1940 and to the output receptacle 1930.

Detail Description Paragraph:

[0108] The second scanning system 2005 includes many of the same features as the first scanning system 2000, such as an input receptacle 2015, a display 2025, a keypad 2045, denomination keys 2075, and a keyboard 2035. The second scanning system 2005, however, is adapted to receive checks into the input receptacle. The checks are then scanned by the scanning system.

Detail Description Paragraph:

[0109] In this embodiment, the invoices and checks are scanned by image scanners in the respective systems 2000, 2005 in the same manner as in FIG. 4. The images obtained from both the first and second scanning systems 2000, 2005 are then transmitted via a communication link 2060 to the first computer 130 as depicted in FIG. 1.

Detail Description Paragraph:

[0110] In an alternative embodiment, the invoices and checks may be inserted into the first scanning system 2000. The second scanning system 2005 may be used to accept documents for depositing, such as currency bills and checks written to the customer.

CLAIMS:

1. An automated payment system for processing payment of an invoice sent from a payee to a customer, wherein the customer has a bank account at a payor bank and the payee has a bank account at a payor bank, the automated payment system comprising: a document scanning system having: an input receptacle for receiving the invoice and a check for an amount drawn on the customer's account, an image scanner, an output receptacle, a transport mechanism adapted to transport the invoice and the check from the input receptacle, past the image scanner, and to the output receptacle, the image scanner being adapted to obtain at least one image of the invoice and at least one image of the check, and a controller coupled to the transport mechanism and the image scanner, the controller adapted to control the transport mechanism and the image scanner; a first computer at the payor bank communicatively coupled to the document scanning system and adapted to receive the at least one image of the check and the at least one image of the invoice, the first computer is further adapted to debit the customer's account for the amount of the check; and a second computer at the payee bank communicatively coupled to the first computer and adapted to receive the at least one image of the check and the at least one image of the invoice from the first computer; wherein the first computer is further adapted to transmit funds in the amount of the check to the payee bank and the second computer is adapted to receive the funds and to credit the payee's account for the amount of the funds.

27. The automated payment system of claim 25, further comprising a second printer adapted to inscribe the check with a transaction amount.

37. The automated payment system of claim 1, wherein the image scanner further comprises: a mirror adapted to receive an image of a first side of the check and invoice; and a single scan head adapted to receive the image of the first side of the check and invoice from the mirror; wherein the single scan head receives an image of the second side of the document.

41. The automated payment system of claim 1, wherein the output receptacle includes a first output bin and a second output bin.

42. The automated payment system of claim 41, wherein one of the first and second output bins is adapted to be an off sort bin to receive at least one of checks and invoices unable to be scanned by the document scanning system.

43. The automated payment system of claim 41, wherein the first output bin is adapted to accept checks and the second output bin is adapted to accept invoices.

48. A method of debiting a first financial account and crediting a second financial account, the first financial account belonging to a customer and the second financial account belonging to a payee, the method comprising: receiving a check drawn on the first financial account in an input receptacle of a document scanning system; receiving an invoice referencing the second financial account in an input receptacle of the document scanning system; transporting the check past an image scanner of the document scanning system; transporting the invoice past the image scanner of the document scanning system; scanning the check and the invoice with the image scanner to generate an electronic image of the check and an electronic image of the invoice; obtaining a transaction amount from the image of the check; obtaining account information from the image of the invoice; transmitting the image of the check and the image of the invoice to a payor financial institution, the financial institution holding the first financial account; debiting the first financial account for the transaction amount; transmitting the image of the check, the image of the invoice, and funds equal to the transaction amount to a payee financial institution, the financial institution holding the second financial account; and crediting the second financial account for the transaction amount.

74. An automated payment system for processing payment of an invoice sent from a payee to a customer, wherein the customer has a bank account at a payor bank and the payee has a bank account at a payor bank, the automated payment system comprising: a document scanning system adapted to obtain at least one image of at least one of the invoice and the check; a first computer at the payor bank communicatively coupled to the document scanning system and adapted to receive the at least one image of at least one of the check and the invoice, the first computer is further adapted to debit the customer's account for the amount of the check; and a second computer at the payee bank communicatively coupled to the first computer and adapted to receive the at least one image of at least one of the check and the invoice from one of the first computer and the document scanning system, the second computer further adapted to credit the payee's account for the amount of the check.

75. A method of debiting a first financial account and crediting a second financial account, the first financial account belonging to a customer and the second financial account belonging to a payee, the method comprising: receiving a check drawn on the first financial account and having a transaction amount in a document scanning system; receiving an invoice referencing the second financial account in the document scanning system; obtaining an image of the check; obtaining an image of the invoice; transmitting the image of the check and the image of the invoice to a payor financial institution, the financial institution holding the first financial account; debiting the first financial account for the transaction amount; transmitting the image of the check to a payee financial institution, the payee financial institution holding the second financial account; and crediting the second financial account for the transaction amount.

76. An automated payment system for processing payment of an invoice sent from a payee to a customer, wherein the customer has a bank account at a payor bank and the payee has a bank account at a payor bank, the automated payment system comprising: a plurality of document scanning systems, each of the document scanning systems adapted to obtain at least one image of at least one of the invoice and the check; a first computer at the payor bank communicatively

coupled to each of the plurality of document scanning systems and adapted to receive the at least one image of at least one of the check and the invoice, the first computer is further adapted to debit the customer's account for the amount of the check; and a second computer at the payee bank communicatively coupled to the first computer and adapted to receive the at least one image of at least one of the check and the invoice from one of the first computer and the document scanning system, the second computer further adapted to credit the payee's account for the amount of the check.

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

[First Hit](#) [Previous Doc](#) [Next Doc](#) [Go to Doc#](#)☐ [Generate Collection](#) [Print](#)

L12: Entry 14 of 94

File: PGPB

Aug 28, 2003

DOCUMENT-IDENTIFIER: US 20030163415 A1

TITLE: System and method for transfer of funds between individualsAbstract Paragraph:

The invention provides a system and method for the transfer of funds between individuals in an efficient, effective and economical manner. The system includes a transmitting data entry device for entering transmitting transfer data identifying a first personal account of a first individual into a transfer coordinator device, and a receiving data entry device for entering receiving transfer data identifying a second personal account of a second individual into the transfer coordinator device. In addition, amount data corresponding to a monetary amount to be transferred from the first personal account of the first individual to a second personal account of a second individual is entered into the transfer coordinator device. A mechanism is provided for transferring the monetary amount from the first personal account to the second personal account based on the transmitting transfer data and the receiving transmitting data entered into the transfer coordinator device.

Classification at Publication, US Primary Class/Subclass:

705/39

Summary of Invention Paragraph:

[0001] The present invention is directed to providing a system and method for transferring monetary funds between individuals in an effective, efficient and economical manner. More specifically, the invention provides a system and method for effectively and efficiently transferring monetary funds between individuals without requiring the use of conventional forms of commercial paper or electronic transfers.

Summary of Invention Paragraph:

[0002] The advent of the Internet has lead the rapid development of direct electronic commerce between individuals. Internet auctions sites, for example, allow an individual to place an item up for sale and to receive bids from individuals located all over the world. Once a successful sale has been completed, however, it is then necessary to find an efficient mechanism for transferring funds directly from the buying individual to the selling individual in a secure manner. In addition, the mechanism for funds transfer must provide the individual receiving payment with a high degree of confidence that the payment is in fact valid.

Summary of Invention Paragraph:

[0003] One could, of course, forward payment in cash to the selling party through conventional mail or private delivery services. Sending cash, however, always entails a certain degree of risk that the payment will be stolen. Further, if the transaction is between individuals in different countries, the monetary units forwarded by the buyer may not be acceptable to the seller, which would require either the buyer or the seller perform a currency conversion to the appropriate monetary units. In addition, cash payments are delayed by the requirement for manual transportation and delivery of the cash payment from the buyer to the seller.

Summary of Invention Paragraph:

[0005] Clearly, it would be advantageous to permit the buyer to transfer funds electronically directly from the buyer's personal account to the personal account of the seller. One conventional mechanism to provide for electronic funds transfer is through the use of a wire transfer, wherein the buyer notifies his bank to electronically transfer funds to the account of the buyer. Again, wire transfer payments are generally not that convenient to make, as the seller must receive the buyer's account information and then must instruct his bank to make payment. In addition, fees for wire transfers (like certified checks and bank checks) are usually too high to be practical for small monetary transactions.

Summary of Invention Paragraph:

[0006] Attempts have been made to develop some form of electronic money to handle small transactions. Many of these systems, however, require both individuals to maintain special accounts, subscribe to a particular service or utilize proprietary transfer techniques in the form of special debit cards. In addition, in many instances it is possible to only transfer funds to individuals that subscribe to the same service.

Summary of Invention Paragraph:

[0009] In view of the above, it would be desirable to provide a system and method that would permit the transfer of funds between individuals in an efficient, effective and economical manner, without the drawbacks associated with cash payments, commercial paper and conventional forms of electronic funds transfer.

Summary of Invention Paragraph:

[0010] The invention provides a system and method that would permit the transfer of funds between individuals in an efficient, effective and economical manner, without the drawbacks associated with cash payments, commercial paper and conventional forms of electronic funds transfer.

Summary of Invention Paragraph:

[0011] Specifically the invention is directed to a system for transferring monetary funds that includes a transmitting data entry device for entering transmitting transfer data identifying a first personal account of a first individual into a transfer coordinator device, and a receiving data entry device for entering receiving transfer data identifying a second personal account of a second individual into the transfer coordinator device. In addition, amount data corresponding to a monetary amount to be transferred from the first personal account of the first individual to a second personal account of a second individual is entered into the transfer coordinator device utilizing at least one of the transmitting data entry device and the receiving data entry device. A mechanism is provided for transferring the monetary amount from the first personal account to the second personal account based on the transmitting transfer data and the receiving transmitting data entered into the transfer coordinator device.

Summary of Invention Paragraph:

[0012] In a preferred embodiment, the first personal account comprises a personal credit card account of the first individual and the second personal account comprises a personal credit card account of the second individual. It will be understood, however, that other types of personal accounts may be readily utilized.

Summary of Invention Paragraph:

[0013] The transmitting transfer data includes account identification data and personal identification data corresponding to the first personal account and the receiving transfer data includes account identification data corresponding to the second personal account.

Summary of Invention Paragraph:

[0015] The file identifier is preferably conveyed to at least one of the first individual and the second individual using electronic mail transfer. Accordingly, the electronic mail address of at least one of the first individual and the second individual is also entered into the transfer coordinator device.

Brief Description of Drawings Paragraph:

[0021] FIG. 3 is a schematic block diagram of a second embodiment of the invention in which remote data entry devices are utilized;

Brief Description of Drawings Paragraph:

[0022] FIG. 4 is a flow diagram illustrating the entry of transfer data by an individual that is transferring funds using the embodiment illustrated in FIG. 3;

Brief Description of Drawings Paragraph:

[0023] FIG. 5 is a flow diagram illustrating the entry of transfer data by an individual that is receiving funds using the embodiment illustrated in FIG. 3; and

Detail Description Paragraph:

[0025] An implementation of a first embodiment of the invention is illustrated in block diagram form in FIG. 1. As shown in FIG. 1, a first individual has a conventional first personal account 10, for example a credit card account, a debit card account, a brokerage account, etc., associated with a conventional financial institution. Similarly, a second individual has a conventional second personal account 12 located in a conventional financial institution. The coordination of the transfer of funds from the first personal account 10 to the second personal account 12 is controlled by a transfer coordinator device 14. A first data entry device 16 is provided to permit the first individual to enter transaction data into the transfer coordinator device 16, which is used by the transfer coordinator device 14 to transfer funds from the first personal account 10 to the second personal account 12.

Detail Description Paragraph:

[0026] The first data entry device 16 may comprise, for example, a personal computer, handheld computer, personal digital assistant, telephone or any other device that permits the first individual to transmit the transaction data to the transfer coordinator device 14. The transfer coordinator device 14 may comprise an computer, server or similar processing device than can control the transfer of funds between the first personal account 110 and the second personal account 12, either by directly controlling the transfer of funds between accounts or indirectly by issuing instructions to processing devices of the institutions in which the personal accounts are held to effect the transfer. The transaction data utilized by the transfer coordinator device 14 includes an account identifier for the first personal account 10 an account identifier for the second personal account 12 and the amount to be transferred.

Detail Description Paragraph:

[0027] As just one example, the first data entry device 16 is a personal computer, the transfer coordinator device 14 is a server located at a facility of an Internet Service Provider (ISP) and the first personal account 10 and the second personal account 12 are respectively credit card accounts located at different financial institutions. An individual uses the first data entry device 16 to connect with the transfer coordinator device 14 via an Internet connection and enters the relevant account information and the amount of funds to be transferred. The transfer coordinator device 14 transmits the transfer data to the financial institution holding the first personal account 10, and the financial institution transfers the funds to the financial institution holding the second personal account 12 using conventional data networks. The amount transferred is debited from the first personal account 10 and credited to the second personal account 12. Accordingly, an individual can directly debit his own personal credit card for funds that are to be paid directly to a credit card account of a second individual.

Detail Description Paragraph:

[0028] FIG. 2 illustrates a simple example of a personal account transfer interface window 18 that would be utilized on a personal computer in order to enter the transfer data. The personal account transfer interface window 18 includes a "Transfer From" data entry block 20 including a transfer account field 22 and a personal identification field (ID) 24, a "Transfer To" data entry block 26 including a receiving account field 28, and a transfer amount field 30. In order to transfer funds, the relevant information into the appropriate fields in both data entry blocks and a transfer button 32 (or similar icon) is clicked in order to initiate the transfer operation. A verification of the completion of the transfer can also be provided if so desired.

Detail Description Paragraph:

[0029] The above-described system provides unique advantages over conventional monetary transfer mechanisms. The individuals are simply charging and receiving credit on their own individual credit card accounts without requiring either individual to become a merchant account holder. The funds are efficiently transferred without the delays associated with cash payments or checks. The individual receiving the funds is guaranteed of the validity of the payment with the credit card issuer having the ultimate responsibility of collecting from the individual transferring the funds. The funds can be transferred anywhere in the world, and automatic exchange rate conversions can be accomplished as is done with conventional credit card transactions. In addition, the architecture is open to either individual being the party that is initiates transfer, namely, it is also possible for the individual that is to receive funds to provide the transfer data to the transfer coordinator device 14 in order to receive funds from the individual that is paying the funds. Alternatively, both individuals may utilize the data entry device 16 to enter their own respective account information.

Detail Description Paragraph:

[0032] One of the main advantages of the invention is the ability to enable transfer of small sums of money conveniently and efficiently between parties that are remotely located from one another. Accordingly, as shown in FIG. 3, the individual receiving the funds can utilize a receiving data entry device 38 that is remote from a transmitting data entry device 40 associated with an individual that is transmitting the funds. The individual transmitting the funds would utilize the transmitting data entry device 40 to access the transfer coordinator device 14 and enter the required transfer data associated with the first personal account 10, while the individual receiving the funds would utilize the receiving data entry device 38 to access the transfer coordinator device 14 and enter the required transfer data associated with the second personal account 12.

Detail Description Paragraph:

[0035] The seller then logs onto the transfer coordinator device 14, enters the file identifier, enters their account information, and hits the transfer button 32. Transfer is then initiated to transfer the funds from the first personal account 10 of the buyer to the second personal account 12 of the seller by the transfer coordinator device 14. For added security, the seller may be required to enter some additional item of information related to the transaction. For example, the seller may be required to also enter the amount of the transaction. Transfer is not initiated if the amount does not match the amount contained in the temporary file for the entered file identifier. FIGS. 4 and 5 are flow diagrams illustrating the above-described process.

Detail Description Paragraph:

[0038] As shown in FIG. 6, a first individual inserts his credit card into an ATM. The card reader in the ATM reads the credit card account information of the first individual and prompts the first individual for an ID. The first individual enters an ID to initiate further action. The ATM then requests the amount of money to be transferred. The first individual enters the amount and the first individual's card is returned. A second individual is then prompted to enter their card which is read by the card reader to obtain the second individual's account information. The second individual is then prompted for their ID. Once the account information is verified, the transaction is initiated to transfer funds from the first individuals personal account to the second individuals personal account.

Detail Description Paragraph:

[0039] It will be understood that ATM's can also be utilized as data entry devices at separate locations in a manner similar to that described with respect to FIG. 3, thereby eliminating the necessity for one or both of the individuals to have Internet access. As ATM's are readily available throughout the world, anyone with a credit card could quickly and efficiently transfer funds by charging their own credit card account and crediting the credit card account of a receiving party.

Detail Description Paragraph:

[0040] The availability of inexpensive credit card readers can even permit the use of readers on personal computing devices. A home personal computer, for example, can be equipped with a credit card reader so that family members may easily transfer funds between one another without requiring manual entry. Alternatively, a dedicated public kiosk including a card reader can be provided as the data entry device to allow individuals to transfer funds between one another at convenient locations such as shopping malls, airports or public arenas.

Detail Description Paragraph:

[0041] The invention has been described in detail with reference to certain preferred embodiments thereof. It will be understood, however, that modifications and variations are possible within the scope of the appended claims. For example, while the illustrated embodiments concentrated on the use of credit card accounts, it will be appreciated that the invention is applicable to permit the direct transfer of funds from any type of personal account of a first individual to any type of personal account of a second individual. The use of established credit card accounts, however, is particularly advantageous due to their ready availability and the infrastructure and architecture that is already in place to allow credit card transactions. Further, while the preferred embodiment utilize computing devices and the Internet to input and transfer data, the invention is applicable to all types of data entry devices and networks. Conventional telephones, for example, may be used to enter account information to a transfer coordinator device either by manual entry or by using voice recognition techniques. Still further, in the embodiment in which the transmitting transfer data and the receiving transfer data are independently entered, the order in which that data is

entered and stored in a temporary file is not significant, namely, either the transmitting transfer data or the receiving transfer data may be entered first.

CLAIMS:

1. A method of transferring monetary funds comprising: entering transmitting transfer data identifying a first personal account of a first individual into a transfer coordinator device utilizing a transmitting data entry device; entering receiving transfer data identifying a second personal account of a second individual into the transfer coordinator device utilizing a receiving data entry device; entering an amount data corresponding to a monetary amount to be transferred from the first personal account of the first individual to a second personal account of a second individual into said transfer coordinator device utilizing at least one of the transmitting data entry device and the receiving data entry device; and transferring the monetary amount from the first personal account to the second personal account based on the transmitting transfer data and the receiving transmitting data entered into the transfer coordinator device.
2. A method of transferring monetary funds as claimed in claim 1, wherein the first personal account comprises a personal credit card account of the first individual and the second personal account comprises a personal credit card account of the second individual.
3. A method of transferring monetary funds as claimed in claim 1, wherein the transmitting transfer data includes account identification data and personal identification data corresponding to the first personal account and the receiving transfer data includes account identification data corresponding to the second personal account.
4. A method of transferring monetary funds as claimed in claim 1, wherein the transmitting transfer data and the receiving transfer data are entered into the transfer coordinator device at different times.
5. A method of transferring monetary funds as claimed in claim 4, further comprising generating a temporary file to temporarily store at least one of the transmitting transfer data and the receiving transfer data and generating a file identifier that corresponds to the temporary file.
6. A method of transferring monetary funds as claimed in claim 5, further comprising conveying the file identifier to at least one of the first individual and the second individual.
7. A method of transferring monetary funds as claimed in claim 5, further comprising accessing the temporary file using the file identifier and matching the transmitting transfer data to the receiving transfer data.
8. A method of transferring monetary funds as claimed in claim 6, wherein the file identifier is conveyed via electronic mail transfer.
9. A method of transferring monetary funds as claimed in claim 8, further comprising entering an electronic mail address of at least one of the first individual and the second individual into the transfer coordinator device.
11. A system for transferring monetary funds comprising: a transmitting data entry means for entering transmitting transfer data identifying a first personal account of a first individual into a transfer coordinator device; a receiving data entry means for entering receiving transfer data identifying a second personal account of a second individual into the transfer coordinator device; wherein amount data corresponding to a monetary amount to be transferred from the first personal account of the first individual to a second personal account of a second individual is entered into said transfer coordinator device utilizing at least one of the transmitting data entry means and the receiving data entry means; and means for transferring the monetary amount from the first personal account to the second personal account based on the transmitting transfer data and the receiving transmitting data entered into the transfer coordinator device.
12. A system for transferring monetary funds as claimed in claim 11, wherein the first personal account comprises a personal credit card account of the first individual and the second personal account comprises a personal credit card account of the second individual.

13. A system for transferring monetary funds as claimed in claim 11, wherein the transmitting transfer data includes account identification data and personal identification data corresponding to the first personal account and the receiving transfer data includes account identification data corresponding to the second personal account.

14. A system for transferring monetary funds as claimed in claim 11, wherein the transmitting transfer data and the receiving transfer data are entered into the transfer coordinator device at different times.

15. A system for transferring monetary funds as claimed in claim 14, further comprising means for generating a temporary file to temporarily store at least one of the transmitting transfer data and the receiving transfer data and means for generating a file identifier that corresponds to the temporary file.

16. A system for transferring monetary funds as claimed in claim 15, further comprising means for conveying the file identifier to at least one of the first individual and the second individual.

17. A system for transferring monetary funds as claimed in claim 15, further comprising means for accessing the temporary file using the file identifier and matching the transmitting transfer data to the receiving transfer data.

18. A system for transferring monetary funds as claimed in claim 16, wherein the file identifier is conveyed via electronic mail transfer.

19. A method of transferring monetary funds as claimed in claim 18, further comprising means for entering an electronic address of at least one of the first individual and the second individual into the transfer coordinator device.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)



Welcome United States Patent and Trademark Office

Search Results

[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)[SUPPORT](#)

Results for "((e-cash)<in>metadata)"

Your search matched 16 of 1278046 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.

e-mail
 printer friendly

» Search Options

[View Session History](#)[New Search](#)

Modify Search

((e-cash)<in>metadata)


☐ Check to search only within this results set

 Display Format: ☒ Citation ☐ Citation & Abstract

» Key

IEEE JNL IEEE Journal or Magazine

IEEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

Select Article Information

**1. The Security Requirement for off-line E-cash system based on IC Card**
 Haeryong Park; Kilsoo Chun; Seungho Ahn;
 Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on
 Volume 2, 20-22 July 2005 Page(s):260 - 264
 Digital Object Identifier 10.1109/ICPADS.2005.279

[AbstractPlus](#) | Full Text: [PDF](#)(144 KB) IEEE CNF
**2. The economics of e-cash**
 ter Maat, M.;
 Spectrum, IEEE
 Volume 34, Issue 2, Feb. 1997 Page(s):68 - 73
 Digital Object Identifier 10.1109/6.570836

[AbstractPlus](#) | Full Text: [PDF](#)(1032 KB) IEEE JNL
**3. Recoverable and untraceable E-cash**
 Liu, J.K.; Wei, V.K.; Wong, S.H.;
 EUROCON'2001, Trends in Communications, International Conference on.
 Volume 1, 4-7 July 2001 Page(s):132 - 135 vol.1
 Digital Object Identifier 10.1109/EURCON.2001.937781

[AbstractPlus](#) | Full Text: [PDF](#)(284 KB) IEEE CNF
**4. How to make e-cash with non-repudiation and anonymity**
 Song, R.; Korba, L.;
 Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International
 Conference on
 Volume 2, 2004 Page(s):167 - 172 Vol.2
 Digital Object Identifier 10.1109/ITCC.2004.1286625

[AbstractPlus](#) | Full Text: [PDF](#)(1371 KB) IEEE CNF
**5. An user efficient fair e-cash scheme with anonymous certificates**
 Pei-Ling Yu; Chin-Laung Lei;
 Electrical and Electronic Technology, 2001. TENCON. Proceedings of IEEE Region 10
 International Conference on
 Volume 1, 19-22 Aug. 2001 Page(s):74 - 77 vol.1
 Digital Object Identifier 10.1109/TENCON.2001.949554

[AbstractPlus](#) | Full Text: [PDF](#)(320 KB) IEEE CNF
**6. A method for imposing spending limit on electronic coins**
 Shek Wong; Wei, V.K.;
 Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on
 16-21 Aug. 1998 Page(s):268
 Digital Object Identifier 10.1109/ISIT.1998.708873

[AbstractPlus](#) | Full Text: [PDF](#)(84 KB) IEEE CNF

- ☐ **7. Traceable e-cash**
Gemmell, P.S.;
Spectrum, IEEE
Volume 34, Issue 2, Feb. 1997 Page(s):35 - 37
Digital Object Identifier 10.1109/6.570827
[AbstractPlus](#) | Full Text: [PDF](#)(380 KB) IEEE JNL

- ☐ **8. Wireless Internet access using anonymous access methods**
Jokela, P.;
Mobile Multimedia Communications, 1999. (MoMuC '99) 1999 IEEE International Workshop on
15-17 Nov. 1999 Page(s):194 - 197
Digital Object Identifier 10.1109/MOMUC.1999.819489
[AbstractPlus](#) | Full Text: [PDF](#)(332 KB) IEEE CNF

- ☐ **9. A study on contents distribution using electronic cash system**
Deok-Gyu Lee; Hyung-Geun Oh; Im-Yeong Lee;
e-Technology, e-Commerce and e-Service, 2004. EEE '04. 2004 IEEE International Conference
on
28-31 March 2004 Page(s):333 - 340
Digital Object Identifier 10.1109/EEE.2004.1287331
[AbstractPlus](#) | Full Text: [PDF](#)(305 KB) IEEE CNF

- ☐ **10. A mobile agent clone detection system with itinerary privacy**
Lam, T.C.; Wei, V.K.;
Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002.
Proceedings. Eleventh IEEE International Workshops on
10-12 June 2002 Page(s):68 - 73
Digital Object Identifier 10.1109/ENABL.2002.1029991
[AbstractPlus](#) | Full Text: [PDF](#)(281 KB) IEEE CNF

- ☐ **11. Distributed electronic payment system based on bank union**
Qiang Xu; Hong Zhao;
High Performance Computing in the Asia-Pacific Region, 2000. Proceedings. The Fourth
International Conference/Exhibition on
Volume 1, 14-17 May 2000 Page(s):548 - 551 vol.1
Digital Object Identifier 10.1109/HPC.2000.846614
[AbstractPlus](#) | Full Text: [PDF](#)(208 KB) IEEE CNF

- ☐ **12. On the security & design of MyKad**
Phan, R.C.-W.; Mohammed, L.A.;
Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on
Volume 2, 21-24 Sept. 2003 Page(s):721 - 724 Vol.2
Digital Object Identifier 10.1109/APCC.2003.1274452
[AbstractPlus](#) | Full Text: [PDF](#)(340 KB) IEEE CNF

- ☐ **13. True anonymity without mixes**
Molina-Jimenez, C.; Marshall, L.;
Internet Applications, 2001. WIAPP 2001. Proceedings. The Second IEEE Workshop on
23-24 July 2001 Page(s):32 - 40
Digital Object Identifier 10.1109/WIAPP.2001.941867
[AbstractPlus](#) | Full Text: [PDF](#)(800 KB) IEEE CNF

- ☐ **14. A scheme for analyzing electronic payment systems**
de Carvalho Ferreira, L.; Dahab, R.;
Computer Security Applications Conference, 1998. Proceedings., 14th Annual
7-11 Dec. 1998 Page(s):137 - 146
Digital Object Identifier 10.1109/CSAC.1998.738600
[AbstractPlus](#) | Full Text: [PDF](#)(100 KB) IEEE CNF



AbstractPlus

BROWSE

SEARCH

IEEE XPLORE GUIDE

SUPPORT

[View Search Results](#) | [Previous Article](#) |

[e-mail](#) [print](#) [friends](#)

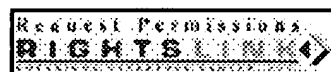
Access this document

 Full Text: [PDF](#) (652 KB)

Download this citation

Choose [Citation](#)Download [EndNote, ProCite, RefMan](#)» [Learn More](#)

Rights & Permissions

» [Learn More](#)

Untraceable off-line electronic cash flow in e-commerce

[Wang, H. Zhang, Y.](#)

Dept. of Math. & Comput., Southern Queensland Univ., Toowoomba, Qld., Australia;

This paper appears in: **Computer Science Conference, 2001. ACSC 2001. Proceedings. 24th Australas:**

Publication Date: 29 Jan-4 Feb 2001

On page(s): 191 - 198

Number of Pages: ix+230

Meeting Date: 01/29/2001 - 02/04/2001

Location: Gold Coast, Qld.

INSPEC Accession Number: 6859685

Digital Object Identifier: 10.1109/ACSC.2001.906642

Posted online: 2002-08-07 00:18:28.0

Abstract

Electronic cash has been playing an important role in electronic commerce. One of the desirable characteristics is its traceability, which can prevent money laundering and can find the destination of suspicious withdrawals. The authors develop a new scheme for untraceable electronic cash, in which the bank involvement in the payment transaction between a user and a receiver is eliminated. The user withdraws electronic "coins" from the bank and uses them to pay to a receiver. The receiver subsequently deposits the coins back to the bank. In the process, the user remains anonymous, unless s/he spends a single coin more than once (double spend). The security of the system is based on DLA (Discrete Logarithm Assumption) and the cut-and-choose methodology

Index Terms

Inspec

Controlled Indexing

[Internet](#) [bank data processing](#) [electronic money](#) [security of data](#)

Non-controlled Indexing

[DLA](#) [Discrete Logarithm Assumption](#) [bank involvement](#) [cut-and-choose methodology](#) [double spend](#) [e-commerce](#) [electronic coins](#) [electronic commerce](#) [money laundering](#) [payment transaction](#) [receiver](#) [suspicious withdrawals](#) [system security](#) [traceability](#) [untraceable e-cash](#) [untraceable electronic cash](#) [untraceable offline electronic cash flow](#)

Author Keywords

Not Available

References

No references available on IEEE Xplore.

Citing Documents

- 1 Achieving secure and flexible M-services through tickets, Hua Wang; Yanchun Zhang; Jinli Cao; Varadharajan, V.
Systems, Man and Cybernetics, Part A, IEEE Transactions on
On page(s): 697- 708, Volume: 33, Issue: 6, Nov. 2003
[Abstract](#) | Full Text: [PDF](#) (494)
- 2 A flexible payment scheme and its role-based access control, Hua Wang; Jinli Cao; Yanchun Zhang
Knowledge and Data Engineering, IEEE Transactions on
On page(s): 425- 436, Volume: 17, Issue: 3, March 2005
[Abstract](#) | Full Text: [PDF](#) (1000)

[View Search Results](#) | [Previous Article](#) |



Untraceable Off-line Electronic Cash Flow in E-Commerce

H. Wang Y. Zhang
Department of Maths & Computing
University of Southern Queensland
Toowoomba QLD 4350 Australia
(wang, yan)@usq.edu.au

Abstract

Electronic cash has been playing an important role in electronic - commerce. One of the desirable characteristics is its traceability, which can prevent money laundering and can find the destination of suspicious withdrawals.

In this paper we develop a new scheme for untraceable electronic cash, in which the bank involvement in the payment transaction between a user and a receiver is eliminated. The user withdraws electronic "coins" from the bank and uses them to pay to a receiver. The receiver subsequently deposits the coins back to the bank. In the process the user remains anonymous, unless s/he spends a single coin more than once (double spend). The security of the system is based on DLA (Discrete Logarithm Assumption) and the cut-and-choose methodology.

Keywords: Electronic-cash, Hash function, Random oracle model, Cut-and-Choose technique, DLA.

1 Introduction

1.1 Electronic Cash and its properties

Traditional cash is a bearer instrument that can be used spontaneously and instantaneously, to make payments from one user to another user without the involvement of a bank. It is the preferred method for low and medium value purchases, and transactions. Cash payments also offer privacy for they are not normally traceable by a third party. Together these factors account for the wide acceptability of traditional cash.

But traditional cash has some shortcomings. First, cash must be created such that is hard to forge and cash must be transported from one place to another place. Cash must be stored safely. Bank notes can be easily destroyed or forged using sophisticated color copier machines. Cash is annoying to carry. It spreads germs, and people can steal it from other people. Another shortcoming of traditional cash is

that of cannot be used for payments over the phone or the Internet.

Cheques and credit cards have reduced cash circulation through out our society, but cheques and credit cards allow people to trace the user's privacy to a degree never imagined before.

Hence, a new "cash" is needed which can allow for authenticated but untraceable messages. For example, Alice can transfer "cash" to Bob. But newspaper reporter Eve does not know Alice's identity. Bob can then deposit that money into his account, and the bank has no idea who Alice is. But if Alice tries to buy cocaine with the same piece of the "cash" she sent to Bob, she will be detected by the bank. And if Bob tries to deposit the same piece of "cash" into two different accounts, he will be detected, but Alice will remain anonymous. It is called Electronic-cash (or E-cash) to differentiate it from digital money with an audit trail, such as cards. Electronic cash can make money laundering more difficult for a coin must run a full cycle from the bank during withdrawal to the same bank for deposit (on Internet). An interesting overview of these issues is available in [9].

The ideal electronic cash system should have the following properties:

1. Anonymous; 2. Revocation; 3. Efficiency; 4. Crime prevention.

Firstly, electronic-cash should be anonymous for legitimate users. The bank cannot link to the legitimate users, but it will identify the double-spenders. Anonymous is only for legal user, so the revocation of anonymity should be done for illegal user.

E-cash system must be efficient. It means not only should tracing (anonymity revocation) be performed efficiently, but the added burden to the basic system should be minimal for all involved parts—trustees, banks, users and shops. In particular, trustees must be involved only when revocation is required and remain off-line otherwise. At last, a cash system must protect all users for their electronic money, sometimes motivating crimes are more serious than other mistakes.

In an on-line electronic-cash system, the banks have to be on-line during the payment to guarantee that the coins received by shops are valid. But the banks to be on-line during the payment are very strict requirement. In an off-line electronic-cash system, the bank needs not to be involved during the payment proceeding. Of course, the double-spent coins cannot be prevented in the payment but the identity of the double spender can be detected in future.

1.2 Off-line Electronic Cash Overview

Off-line anonymous electronic cash was introduced by Chaum, Fiat and Naor [7]. The security of their scheme relied on some arbitrary assumptions. However, no formal proof was attempted. Although hardly practical, their system demonstrated how off-line e-cash can be constructed and laid the foundation for more secure and efficient schemes to follow.

Okamoto and Ohta [13] were the first to attempt an improvement on this system. They modified the model by moving the most complex part of the functionality of the withdrawal protocol, namely the zero-knowledge proof of the user's identity, to the user setup (account establishment) protocol, which was executed much less frequently. The system relies on more reasonable and clarified assumptions but, it is faster than [7], at least when the account establishment protocol is performed infrequently; otherwise no improvement is claimed.

In 1991, Pfitzmann and Waidner [14] presented a way to base on-line electronic cash on general two-party computation protocols and zero-knowledge proofs. To combine the security of [14] with the relative efficiency of regular cut-and-choose systems, Franklin and Yung [10] presented a provably secure scheme that was not based on general computation protocols. The security relied on the DLA and on the existence of a mutually trusted party (equivalently, a general computation protocol could substitute the trusted party's functionality). Although a cut-and-choose techniques were used and its efficiency was still not a prime consideration, Franklin and Yung were the first to illustrate how off-line e-cash could be based on the DLA, as well as the first to construct a formal security model; variations of this security model have appeared in subsequent e-cash systems [6, 12].

1995, Chan, Frankel and Tsionis [6] presented a provably secure off-line e-cash scheme that relied only on the security of RSA. This cut-and-choose based scheme extended the work of Franklin and Yung [10] who aimed to achieve provable security without the use of general computation protocols. In 1998, T. Yiannis and M. Yung [22] showed that the decision Diffie-Hellman assumption implies the security of the original ElGamal encryption scheme (with messages from a subgroup) without modification and they

also showed that the opposite direction holds, i.e., the semantic security of the ElGamal encryption was actually equivalent to the decision Diffie-Hellman problem.

1.3 Outline of the paper

In this paper, we propose an untraceable, off-line electronic cash scheme which achieves provable security without the use of general computation protocols and without the requirement of a trusted third party, or of a costly general computation-based initialization procedure. To illustrate the practicality of schemes that are not based on general computation protocols, and show how to derive an efficient variant based on the random-oracle model; this variant thus achieves provable security based on DLA, cut-and-choose technique and the existence of random oracle like hash functions. Further more our untraceable electronic cash scheme is much more simple than [10]. An implication of it is that truly anonymous e-cash can be implemented very efficiently without sacrificing security in comparison to existing account-based or anonymous-like systems.

This paper is organized as follows: in section 2, some basic definitions and the simple examples are reviewed. The basic model of electronic cash is presented in section 3. In section 4, a new off-line electronic cash scheme is designed and the security analysis of our scheme is given in section 5. A simple example is given in section 6 and the comparison with other scheme is present in section 7, finally the conclusions are included in section 8.

2 Some Basic Definitions

2.1 Hash functions and random oracle model

$h(x)$ is a hash function if and only if given a value x it is computationally hard to find a $y \neq x$ such that $h(x) = h(y)$, i.e., collisions are hard to find.

Hash functions are a major building block for several cryptographic protocols, including pseudorandom generators [1, 3], digital signatures [4], and message authentication.

Hash functions have been used in computer science for a long time. A hash function is a function, mathematical or otherwise, that takes a variable-length input string and converts it to a fixed-length (generally smaller) output string. Regardless of the nature of the function, an adversary can always select values at random from the domain of the function in the hope that they hash on the same value. Counter-intuitively, it can be shown that if the range of a hash function is of size n , a guessing algorithm does not need to perform 2^{n-1} iterations (on average) in order to find a collision, but rather only $O(2^{n/2})$. Currently, a range of 160 bits is considered to be sufficient for most applications.

A random oracle R is a mapping (function) from $\{0,1\}^* \rightarrow \{0,1\}^\infty$ chosen by selecting each bit of $R(x)$ uniformly and independently (random and unpredictable), for every x .

Random oracles are very powerful tools, allowing the construction of very efficient signatures.

A system model is called a random oracle model if its operations are under random oracles. In this model, the functions (random oracles) produce a random answer for each new query. Of course, if the same query is asked twice, identical answers are obtained. Random oracle models are commonly used in practice and in electronic cash in particular [2, 5, 11], especially in light of a construction by Bellare and Rogaway [6] showing instantiations of random oracles based on efficient hash function, such as MD5 [17].

For example, suppose $h' : \{0,1\}^{256} \rightarrow \{0,1\}^{64}$ is a hash function, $h''(x) = h'(x) \oplus C$, where C is a random chosen 64 bit constant and \oplus denotes bitwise exclusive or. Defining $h_1(x) = h''(x[0]) || h''(x[1]) || h''(x[2]) || \dots$, where $|x| = 224$ and $[i]$ is the encoding of i such that $x[i]$ has 256 bits, where $||$ denote concatenation. We define $h : \{0,1\}^* \rightarrow \{0,1\}^\infty$ as follows: for any input x , encoding x by x' consisting of x , the bit "1" and "0" to make $|x'|$ a multiple of 224 bits (the "1" and "0" are depended on the encoding). Now let $x' = x'_1 || \dots || x'_n$, where $|x'_i| = 224$ and define $h(x) = h_1(x'_1) \oplus \dots \oplus h_1(x'_n)$. Then $h(x)$ is a random oracle for its output is random and unpredictable.

2.2 Cut-and-Choose technique

Cut-and-Choose technique is a basic method in integer theory. We can use mathematic method to express cut-and-choose technique. Suppose a set $A = \{1, 2, \dots, 2k\}$.

1. Alice cuts the set A into two parts

$$A_1 = \{j_1, \dots, j_k\}, A_2 = A - A_1$$

the size of A_1 is same as that of A_2 .

2. Bob randomly chooses A_1 , or A_2 .
3. Alice gets the remain part.

The cut-and-choose technique works for no way but Alice can guess which part Bob will choose. Alice has a 50 percent chance of guessing which party Bob will choose in each round of the protocol, so she has a 50 percent chance of right guess. Her chance to be right in two rounds is 25 percent, and the chance of her to be right all n times is 2^{-n} . After 16 rounds, the right rate of Alice's guessing is 1 in 65536. So Alice cannot get anything but guessing. It means Alice gets nothing and it is called zero-knowledge.

Michael Rabin was the first person to use the cut-and-choose technique in cryptography [15].

The first e-cash systems employed a cut-and-choose technique: at withdrawal the user presents $2n$ (where n is the security parameter) "terms"; the bank "cuts-and-chooses" n , for which the user reveals the inner structure. The bank verifies their correctness and blindly signs the remaining n . At payment a similar cut-and-choose technique is employed for the shop to verify a "hint" on the user's identity, such that upon double-spending two hints identify the user. The cut-and-choose technique is a tool for a zero-knowledge proof of correctness of the coin, thus preserving user anonymity. Security is guaranteed with probability overwhelming in n , but a scheme's communication, computation and storage requirements are multiplied by a factor of n .

2.3 RSA and DLA

RSA is a public-key cryptosystem that offers both encryption and digital signatures (authentication). Ron Rivest, Adi Shamir and Leonard Adleman developed RSA in 1977 [16].

RSA works as follows: take two large primes p and q , and compute their product $n = pq$; n is called the modulus. Choose a number e , less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1. Find another number d such that $(ed-1)$ is divisible by $(p-1)(q-1)$. The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e) , the private key is d . It is currently difficult to obtain the private key d from the public key (n, e) .

The source of DLA is the discrete logarithm problem.

The discrete logarithm problem is as follows: given an element g in a group G of order t , and another element y of G , the problem is to find x , where $0 < x < t-1$, such that y is the result of composing g with itself x times. In some groups there exist elements that can generate all the elements of G by exponentiation (i.e., applying the group operation repeatedly) with all the integers from 0 to $t-1$. When this occurs, the element is called a generator and the group is called cyclic. Rivest [17] has analyzed the expected time to solve the discrete logarithm problem both in terms of computing power and cost.

Discrete Logarithm Assumption (DLA) is an assumption that the discrete logarithm problem is believed to be difficult and also to be the hard direction of a one-way function. For this reason, it has been used for the basis of several public-key cryptosystems, including the famous ElGamal system.

2.4 Blind signature

Blind signature schemes, first introduced by Chaum [7] allow a person to get a message signed by another party

without revealing any information about the message to the other party.

Suppose Alice has a message m that she wishes to have it signed by Bob, and she does not want Bob to learn anything about m . Let (n, e) be Bob's public key and d be his private key. Alice generates a random value r such that $\gcd(r, n) = 1$ and sends $m' = r^e m \pmod{n}$ to Bob. The value m' is "blinded" by the random value r , and hence Bob can derive no useful information from it. Bob returns the signed value, $s' = (m')^d = (r^e m)^d \pmod{n}$ to Alice. Since $s' = r m^d \pmod{n}$, Alice can obtain the true signature s of m by computing $s = s' r^{-1} \pmod{n}$.

A probabilistic polynomial time (p.p.t) Turing machine M is a Turing machine which can flip coins as an additional primitive step, and on input string x runs for at most a polynomial in $|x|$ steps. $M(x, y)$ denotes the outcome of M on input x when internal coin tosses are y .

3 Basic model

Electronic cash (in particular off-line untraceable electronic cash) has sparked wide interest among cryptographers ([9, 20, 17, 21, 12], etc.). In its simplest form, an e-cash system consists of three parts (a bank B , a user U and a shop S) and three main procedures as shown in Figure 1 (withdrawal, payment and deposit). In a coin's life-cycle, the user U first performs an account establishment protocol to open an account with the bank B . To obtain a coin U performs a withdrawal protocol with B and during a purchase U spends a coin by participating in a payment protocol with the shop S . To deposit a coin, S performs a deposit protocol with the bank B .

Users and shops maintain an account with the bank, while

1. U withdraws electronic coins from his account, by performing a withdrawal protocol with the bank B over an authenticated channel.
2. U spends a coin by participating in a payment protocol with a shop S over an anonymous channel, and
3. S performs a deposit protocol with the bank B , to deposit the user's coin into his account.

The system is *off-line* if during payment the shop S does not communicate with the bank B . It is *untraceable* if there is no p.p.t. TM (probabilistic polynomial-time Turing Machine) M access to all bank's views of withdrawal, payment and deposit protocols, can decide a coin's origin. It is *anonymous* if the bank B , in collaboration with the shop S , cannot trace the coin to the user. However, in the absence of tamper-proof hardware, electronic coins can be copied and spent multiple times by the user U . This has been traditionally referred to as double-spending. In anonymous

on-line e-cash, double-spending is prevented by having the bank check if the coin has been deposited before. In off-line anonymous e-cash, however, this solution is not possible; instead, as proposed by Chaum, Fiat and Naor [7], the system guarantees that if a coin is double-spent the user's identity is revealed with overwhelming probability.

There are also three additional proceedings such as the bank setup, the shop setup, and the user setup (account opening). They describe the system initialization, namely creation and posting of public keys and opening of bank accounts. Although they are certainly parts of a complete system, these are often omitted as their functionalities can be easily inferred from the description of the three main procedures. For clarity we will only describe the bank setup and the user setup (because the shop setup is as similar as user setup) for our new scheme in the next section.

4 New off-Line Untraceable Electronic Cash Scheme

In this section, we propose a new off-line untraceable electronic cash scheme.

Our scheme includes two basic processes in system initialization (bank setup and user setup) and three main protocols: a new withdrawal protocol with which U withdraws electronic coins from B while his account is debited, a new payment protocol with which U pays the coin to S , and a new deposit protocol with which S deposits the coin to B and has his account credited.

4.1 System Initialization

We only describe the bank setup and the user setup based on Discrete Logarithm Assumption and random-oracle model here and omit the detail of the shop setup (because the shop setup is similar to the user setup).

Bank's setup: (performed once by B)

Primes p and q are chosen such that $|p - 1| = \delta + k$ for a specified constant δ , and $p = \gamma q + 1$, for a specified small integer γ . Then a unique subgroup G_q of prime order q of the multiplicative group Z_p and generators g, g_1, g_2 of G_q are defined. Secret key $x_B \in_R Z_q$ for a denomination is created, where $a \in_R A$ means that the element a is selected randomly from the set A with uniform distribution. Hash function H from a family of collision intractable (or, ideally, according to [9], correlation-free one way) hash function is also defined. B publishes p, q, g, g_1, g_2, H and its public keys $h = g^{x_B} \pmod{p}$, $h_1 = g_1^{x_B} \pmod{p}$, $h_2 = g_2^{x_B} \pmod{p}$.

The secret key x_B is safety under the DLA. The Hash function will be used in withdrawal process.

User's setup (account opening): (performed for each user U)

The bank B associates the user U with $I = g_1^{u_1} \pmod{p}$ where $u_1 \in G_q$ is generated by U and $g_1^{u_1} g_2 \neq 1 \pmod{p}$. U computes $z = h_1^{u_1} h_2 = (I g_2)^{x_B} \pmod{p}$.

In system initialization, the communication complexity is $O(l)$ for the user only sends its account I of length l bits to the bank, and the computation complexity is $O(1)$.

After the user's account and the shop's account opening, we can describe the new untraceable electronic cash scheme.

4.2 New Untraceable Electronic Cash Scheme

We now describe the new off-line untraceable electronic cash scheme which includes three protocols: withdrawal protocol, payment protocol and deposit protocol.

Withdrawal: (over an authenticated channel between B and U)

The withdrawal creates a "restrictively blind" signature B_i ($i = 1, \dots, k$) of I and using cut-and-choose technology. U will put a signature as $(I g_2)^s$ where s is a random number (chosen by U and kept secret).

1. The user chooses a_i, c_i , $1 \leq i \leq k$, independently and uniformly at random from the residues \pmod{p} .
2. The user forms and sends to the bank k blinded candidates $B_i = H(x_i, y_i) \pmod{p}$, $1 \leq i \leq k$, where

$$x_i = g^{a_i} \pmod{p}, y_i = g_1^{a_i \oplus (I \| c_i)} \pmod{p}.$$

3. The bank chooses a random subset of $k/2$ blinded candidate indices

$$R = \{i_j\}, 1 \leq i_j \leq k, 1 \leq j \leq k/2$$

and transmits it to the user.

4. The user transmits $A = (I g_2)^s \pmod{p}$ and $z' = z^s \pmod{p}$ to bank.
5. The user displays a_i, c_i values for all i in R , and the bank checks them. To simplify notation we assume that $R = \{k/2 + 1, k/2 + 2, \dots, k\}$.
6. The bank verifies: $A^{z_B} = z' \pmod{p}$ and gives the user the electronic coin C ,

$$C = \prod_{i \notin R} B_i = \prod_{1 \leq i \leq k/2} B_i \pmod{p}.$$

We use the Hash function in step 2 and the cut-and-choose technique in step 3, step 5 and step 6. The basic safety in withdrawal is protected by Hash function, and

the deep safety is kept by the cut-and-choose technique. Indeed, since cut-and-choose technique is zero-knowledge proof, then nothing can be inferred about the coin. At the final step, the output of the coin is random and unpredictable. It is a random oracle model and secure in withdrawal.

In withdrawal process, the communication complexity is $O(k)$ for the user sends B_i , $1 \leq i \leq k$ to the bank and the bank sends R which length is $k/2$ to the user, the computation complexity is $O(q^{k/2})$, since x_i, y_i, B_i, A, Z', C must be computed. $C = \prod_{1 \leq i \leq k/2} B_i \pmod{p}$ is the main computation.

Payment: (performed between the user and the shop over an anonymous channel)

At payment time the user supplies information to the receiver (which is later forwarded to the bank) so that if a coin is double-spent the user is identified. The detailed payment is as below. (the user and the shop agree on date/time):

1. The user sends C to the shop.
2. The shop chooses a random binary string $z_1, z_2, \dots, z_{k/2}$, and sends to the user.
3. The user responds as follows, for all $1 \leq i \leq k/2$:
 - a. If $z_i = 1$, then sends to the shop: a_i, y_i
 - b. If $z_i = 0$, then sends the shop: $x_i, a_i \oplus (I \| c_i), c_i$
4. The shop verifies that C is right since the user's responses can fit C .

The user gives some data to the shop according its random binary string $z_1, z_2, \dots, z_{k/2}$. The random binary strings from different shops are different with high probability. Two different shops will send to the user complementary binary values for at least one bit z_i for which B_i was of the proper form. The user's account I can be obtained from $a_i, y_i, x_i, a_j \oplus (I \| c_j), c_j$ when $i = j$. The different strings will be gotten if the user uses the same coin C twice, then the user has a high probability of being traced.

In payment, the communication complexity is $O(k + l)$ for the shop sends z_i , $1 \leq i \leq k/2$ to the user and the user sends responds $a_i, y_i, x_i, a_i \oplus (I \| c_i), c_i$ to the shop. The computation complexity is $O(1)$ for only the shop verifies the form C .

Deposit: (The receiver deposits a coin to a bank)

After some delay for the system is off-line, the shop sends to B the payment transcript, consist of $C, a_i, y_i, x_i, a_j \oplus (I \| c_j), c_j$ and the date/ time of the transaction. The bank verifies their correctness and credits his account.

In deposit, the communication complexity is $O(k + l)$ for the shop sends user's responds $a_i, y_i, x_i, a_i \oplus (I \| c_i), c_i$ to the bank. The computation complexity is $O(1)$, since only the bank verifies whether C was used before or not.

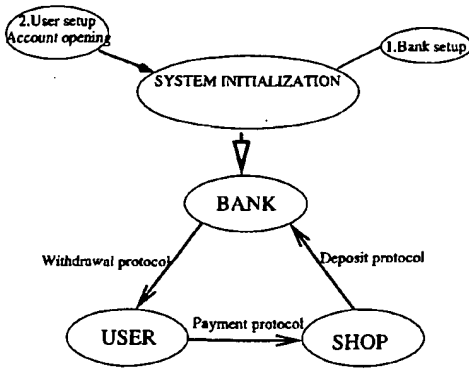


Figure 1. Basic off-line electronic cash system

Remark The receiver (shop) deposits the coin in its account provided by the bank with a transcript of the payment. If the user uses the same coin C twice, then the user has a high probability of being traced: with high probability, two different receivers will send complementary binary values for at least one bit z_i for which B_i was of the proper form. The bank can easily search its records to ensure that C has not been used before. If the user uses C twice, then with high probability, the bank has both $a_i, a_i \oplus (I||c_i)$ and c_i with same i . Thus, the bank can isolate the user and trace the payment to the user's account I .

In our new scheme, the communication complexity is $O(k+l)$ and the computation complexity is $O(q^{k/2})$ where k is the security parameter and l is the size of user's identity I .

The system initialization in figure 1 includes the security random oracle model and how to get the bank setup and the user setup. It is important for the withdrawal, payment and deposit in our new scheme. The security of our new scheme is also based on the system initialization.

We have shown how to derive an efficient scheme based on the random-oracle model. It achieves provable security based on DLA and the existence of random oracle like hash functions. Based on this system initialization, three new protocols with cut-and-choose methodology are designed. It is much more secure due to the cut-and-choose methodology and random-oracle model.

5 Security Analysis

An off-line E-cash scheme is secure [10] if the following requirements are satisfied:

1. *Unreusable*: If any user uses the same coin twice, the identity of the user's can be computed.

2. *Unexpandable*: With n withdrawal proceedings, no p.p.t. (Probabilistic polynomial time) Turing Machine can compute $(n+1)$ th distinct and valid coin.
3. *Unforgeable*: With any numbers of the customer's withdrawal, payment and deposit, no p.p.t. Turing Machine can compute a single valid coin.
4. *Untraceable*: With any numbers of the customer's valid withdrawal, payment and deposit protocols, no p.p.t. Turing Machine can compute a legal user's identity.

We employ Discrete Logarithm methods in our new scheme; these methods have been suggested in many of the recent e-cash schemes to bind identities (an unavoidable issue in off-line e-cash). These methods were started in [14] and continued by others [6, 12] as well as in [21]. The security of our scheme is based on the hardness of Discrete Logarithms [22] and the cut-and-choose technology. The cut-and-choose technology is based on zero-knowledge proof, and the scheme assumes that the hash function used is perfect (i.e., random oracles).

We have analysed the untraceability and unreuseability before. To prevent the cooperation of the bank and some others frame the user as a multiple spender in the scheme, we use digital signature Z^s for s is known only by the user. To prevent unexpanding, we use the Discrete Logarithm methods and cut-and-choose technology.

A possible problem with the scheme is a collusion between a user U and the second shopkeeper. After having user transactions with two receivers which send the same information to the bank, the bank knows that with high probability one of them is lying, and the bank can decide the first purchase is right by the date/time in the payment but cannot trace the coin to the user's account.

To prevent the bank frame the user as a multiple spender in the scheme, we use digital signature Z^s for s is known only by the user. The user is protected against frame-up only computationally, not unconditionally.

6 A simple example

We will give a simple example to explain how our scheme works in this section.

Bank setup

Suppose $(p, q, \gamma, k) = (47, 23, 2, 4)$, then $G_q = \{0, 1, 2, \dots, 22\}$ is a subgroup of order 23. $g = 2, g_1 = 3, g_2 = 5$ are the generators of G_q . Bank's secret key $x_B = 4$ and hash function $H(x, y) = 3^x * 5^y \pmod{47}$. Bank publishes $H(x, y)$ and $\{p, q, g, g_1, g_2, h, h_1, h_2\} = \{47, 23, 2, 3, 5, 16, 34, 14\}$.

User setup (opening an account)

Every user has a secret key. We assume the secret of a user is $u_1 = 7$ and the user sends $I = g_1^{u_1} = 32 \pmod{47}$ to the bank. The user computes

$$z = h_1^{u_1} * h_2 = 18 \pmod{47}.$$

The user will perform the following steps when s/he does shopping.

1. Withdrawal

The user chooses a one-time secret key $s = 3$ and

(a) Chooses

$$\{a_1, a_2, a_3, a_4, c_1, c_2, c_3, c_4\} = \{1, 2, 3, 4, 11, 12, 13, 14\}$$

(b) The user computes (We omit module 47):

$$\{a_1, a_2, a_3, a_4, v_1, v_2, v_3, v_4\} = \{2, 4, 8, 16, 32, 7, 7, 32\}$$

and sends B_i to the Bank:

$$\{B_1, B_2, B_3, B_4\} = \{16, 45, 26, 36\}.$$

(c) The Bank chooses $R = \{3, 4\}$ (suppose) and sends it to the user.

(d) The user transmits $A = (Ig_2)^s = 44 \pmod{47}$ and $z' = z^s = 4 \pmod{47}$ to the Bank.

(e) The user displays $(a_3, a_4, c_3, c_4) = (3, 4, 13, 14)$ to the Bank, and The Bank checks the correctness of the B_3, B_4 .

(f) The Bank verifies $A^{z'} = 44^4 = 34 = z' \pmod{47}$ and gives the user the coin C :

$$C = B_1 * B_2 = 16 * 45 = 15 \pmod{47}.$$

2. Payment

The user can use the coin in shop as follows. If the user uses the coin only once, she is legal. But when she uses the coin twice she will be identified.

(a) The user sends $c = 15$ to a shop (The user needs not to display I).

(b) The shop chooses a random binary string to the user, suppose it is $\{z_1, z_2\} = \{1, 0\}$.

(c) The user responds to the shop $(a_1, y_1) = (1, 32)$ for $z_1 = 1$ and $(x_2, c_2, a_2 \oplus (I||c_2)) = (4, 12, 526)$ for $z_2 = 0$.

(d) The shop sends the responds $(a_1, y_1, x_2, c_2, a_2 \oplus (I||c_2))$ to the bank and the bank checks if the responds are correct with $\{B_1, B_2\} = \{16, 45\}$.

3. Deposit and owner tracing

The bank will put the money into the shop's account when the checking of the coin C is correct. The shop can also see that the money in his account is added. If the user uses the coin twice, the bank will get $a_i, a_j \oplus (I||c_j)$ and c_j with $i = j$, then the user's identity I can be found.

7 Comparisons

In this section, we compare our new scheme with of the proposed approach by M. Franklin and Yung [10]. We will see that the communication complexity and computation complexity of our protocols are better than that in [10].

We first recall the basic main processing stages of M. Franklin and M. Yung [10].

1. $R \rightarrow A : Z_1^* = \rho_1^{e_A} h(z_1) \pmod{N_A}, \dots, Z_{2k}^* = \rho_{2k}^{e_A} h(z_{2k}) \pmod{N_A}$, where

(a) $\rho_i \in_R Z_{N_A}^*$ for all $1 \leq i \leq 2k$.

(b) $z_i = e'(s, r_i)$ for all $1 \leq i \leq 2k$, where each r_i is uniformly random over the appropriate range, and where e' is a public and easily computable function.

(c) h is a publicly known collision-free hash function.

2. In round two, the following messages are sent:

(a) $R \rightarrow A : [r_i, \rho_i : i \in S]$.

(b) $A \rightarrow R : C' = \prod_{j \notin S} (z_j^*)^{d_A} \pmod{N_A}$, assuming that the messages received so far are consistent (otherwise A terminates the protocol); i.e.:

$$z_j^* \rho_j^{-e_A} = h(e'(s, r_j)) \quad j \in S.$$

3. R finds $[r, C]$ where

(a) $r = [r_j : j \notin S]$

(b) $C = C' \prod_{j \notin S} \rho_j^{-1} \pmod{N_A}$

(c) The public and easily computable function e is defined to be.

$$e(s, r) = [e'(s, r[1]), \dots, e'(s, r[k])].$$

Where e_A, d_A is A 's encryption and decryption key, respectively. e_A is public and d_A is secret key. N_A is public.

In [10], the communication complexity is $O(k^2 l)$ bits where k is a security parameter and l is the size of a signed bit; the computation complexity is $O(n^{k/2})$. In our case, the communication complexity is $O(k + l)$. The computation complexity is $O(q^{k/2})$. As general, $q < n$.

	communication complexity	Computation complexity
[10]	$O(k^2 l)$	$O(n^{k/2})$
New scheme	$O(k + l)$	$O(q^{k/2})$

8 Conclusion

In this paper an untraceable electronic cash scheme is designed which is an off-line scheme and without using of general computation protocols and without the requirement of a trusted party. We have shown how to derive an efficient cash scheme based on the variants in the random-oracle model. The variants thus achieve provable security based on DLA and the existence of random oracle like hash function. The security of the system is based on DLA and the cut-and-choose methodology. We give a simple example to explain our new untraceable scheme, and finally, we compare it with the other scheme used cut-and-choose technique.

References

- [1] Bellare M., Goldreich O., and Krawczyk H. Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier. In *Advances in Cryptology - Crypto 99*, volume 1666 of *Lectures Notes in Computer Science*. Springer-Verlag, 1999.
- [2] Bellare M., Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols. In *First ACM Conference on Computer and Communications Security*, pages 62–73. IEEE, 1993.
- [3] Boyko V., Peinado M., and Venkatesan R. Speeding up Discrete Log and Factoring Based Schemes via Precomputations. In *Advances in Cryptology - Eurocrypt'98*, volume 1807 of *Lectures Notes in Computer Science*. Springer-Verlag, 1998.
- [4] Canetti R., Goldreich O., and Halevi S. The Random Oracle Methodology. In *Proceedings of the 30th ACM STOC '98*, pages 209–218. IEEE, 1998.
- [5] Canetti R., Micciancio D., and Reingold O. Perfectly One-Way Probabilistic Hash Functions. In *Proceedings of the 30th ACM STOC '98*. IEEE, 1998.
- [6] Chan A., Frankel Y., and Tsiounis Y. An efficient off-line electronic cash scheme as secure as RSA. Research report nu-ccs-96-03, Northeastern University, Boston, Massachusetts, 1995.
- [7] Chaum D., Fiat A., and Naor M. Untraceable electronic cash. In *Advances in Cryptology - Crypto 88*, volume 403 of *Lectures Notes in Computer Science*, pages 319–327. Springer-Verlag, 1990.
- [8] Eng T., Okamoto T. Single-trem divisible electronic coins. In *Advances in cryptology-Eurocrypt'94*, volume 950 of *Lectures Notes in Computer Science*, pages 306–319. Springer-Verlag, 1995.
- [9] Frankel Y., Yiannis T., and Yung M. Indirect Discourse Proofs: Achieving Fair Off-Line Electronic Cash. In *Advances in cryptology-Asiacrypt'96*, volume 1163 of *Lectures Notes in Computer Science*, pages 286–300. Springer-Verlag, 1996.
- [10] Franklin M., Yung M. Secure and efficient off-line digital money. In *Proc. of the twentieth International Colloquium on Automata, Languages and Programming*, volume 700 of *Lectures Notes in Computer Science*, pages 265–276. Springer-Verlag, 1993.
- [11] Goldreich O., Krawczyk H. On the composition of zero-knowledge proof systems. *SIAM Journal on Computing*, 25(1):159–192, February 1996.
- [12] Okamoto T. An efficient divisible electronic cash scheme. In *Advances in cryptology-Crypto'95*, volume 963 of *Lectures Notes in Computer Science*, pages 438–451. Springer-Verlag, 1995.
- [13] Okamoto T., Ohta K. Disposable zero-knowledge authentication and their applications to untraceable electronic cash. In *Advances in Cryptology - Crypto'89*, volume 435 of *Lectures Notes in Computer Science*, pages 481–496. Springer-Verlag, 1990.
- [14] Pfizmann B., Waidner M. How to break and repair a 'provably secure' untraceable payment system. In *Advances in Cryptology - Crypto'91*, volume 576 of *Lectures Notes in Computer Science*, pages 338–350. Springer-Verlag, 1992.
- [15] Rabin M. *Digital Signatures, Foundations of secure communication*. New York: Academic Press, New York, 1978.
- [16] Rivest R. L., Shamir A., and Adleman L. M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
- [17] Rivest R. T. The MD5 Message Digest Algorithm. Internet RFC 1321, April 1992.
- [18] Simon D. Anonymous communication and anonymous cash. In *Advances in Cryptology - Crypto'96*, volume 1109 of *Lectures Notes in Computer Science*, pages 61–73. Springer-Verlag, 1997.
- [19] Wang H., Zhang Y. A Protocol for Untraceable Electronic Cash. In *Proceedings of the First International Conference on Web-Age Information Management*, volume 1846 of *Lectures Notes in Computer Science*, pages 189–197. Springer-Verlag, 2000.
- [20] Yacobi Y. Efficient electronic money. In *Advances in cryptology-Asiacrypt'94*, volume 917 of *Lectures Notes in Computer Science*, pages 153–163. Springer-Verlag, 1995.
- [21] Yiannis T. Fair Off-Line Cash made easy. In *Advances in cryptology-Asiacrypt'98*, volume 1346 of *Lectures Notes in Computer Science*, pages 240–252. Springer-Verlag, 1998.
- [22] Yiannis T., Yung M. On the security of ElGamal-based encryption. In *International Workshop on Practice and Theory in Public Key Cryptography (PKC '98)*, volume 1346 of *Lectures Notes in Computer Science*, Yokohama, Japan, 1998. Springer-Verlag.

An User Efficient Fair E-cash Scheme with Anonymous Certificates

Pei-Ling Yu, *Nonmember*, and Chin-Laung Lei, *Member, IEEE*

Abstract—E-cash is considered as one of the coming mainstreams of digital currency due to its excellent security properties. With its perfect anonymity, however, e-cash may be misused to commit crimes. In this paper, we propose a fair e-cash scheme, which improves the previous schemes by reducing the computational and storage overhead of the trusted third party. In addition, our proposed scheme also possesses the desired user efficient property where a customer only has to compute several modular multiplication and addition in coin withdrawing. Due to the rapidly growing of the Internet access via mobile units with low computation power, the user efficient property is of great worth. Thus this work can provide an efficient and practical payment mechanism for electronic commerce.

Index Terms—electronic cash, electronic commerce, network security, payment.

I. INTRODUCTION

DUE to the rapid development of computer and communication technologies, electronic commerce (EC or eCommerce) has profoundly affected our economic system. Recently, mobile commerce (MC or Mobile eCommerce) becomes the focus of attention because of its more anytime and anywhere flexibility. Nonetheless, a secure, efficient, and convenient payment system is still a desideratum.

Untraceable e-cash [2] is considered as one of the coming mainstreams of digital currency due to its excellent security properties. However, the perfect anonymity property of e-cash may be misused to commit crimes, such as blackmailing and money laundry [10]. As a result, fairness becomes an critical issue of e-cash. With fairness property, the anonymity of e-cash can be revoked with a trusted third party's assistance when illegal activities have been found. On the other hand, customers' privacy should be well protected as long as they perform properly.

In [4], Fan and Lei proposed an user efficient e-cash scheme based on quadratic residual problem. In this scheme, customers only have to compute several modular

multiplications and additions when they withdraw an e-cash coin from the bank. This property becomes more and more valuable recently due to the oncoming trend of mobile commerce. In mobile commerce scenario, customers usually conduct their business with a handheld device, such as smart card, smart phone, or some WAP-enable mobile unit. These mobile devices usually possess merely limited computing power and storage space.

In [3], Fan and Lei proposed an user efficient fair e-cash scheme based on [4]. However, this fair e-cash signature scheme requests an on-line trusted third party. Moreover, the trusted third party has to record several items in its database for each e-cash coin. It may form an intolerable overhead for the trusted third party when the amount of issued coins grows larger and larger.

In this paper, we propose a fair e-cash scheme based on Fan and Lei's work [4]. In our scheme, the trusted third party need not record any thing for each coin. Furthermore, the trusted third party is only involved when customers request anonymous certificates and hence is off-line in e-cash withdraw procedure.

The rest of this paper is organized as follows. Section 2 briefly describes the Fan and Lei's user efficient fair blind signature scheme [3]. Section 3 details our proposed fair e-cash scheme. Then section 4 analyzes the correctness and various properties of our scheme. Finally, conclusions are given in section 5.

II. PRELIMINARY

In Fan and Lei's scheme [3], there are four roles involved, including a bank, a customer, a shop, and a judge (a trusted third party).

The strategy to achieve fairness in [3] is very trivial: the random numbers used in withdraw protocol are selected by the judge instead of the customer himself, so the anonymity of the e-cash coin can be revoked with the judge's assistance when necessary. In the following subsections, the details of Fan and Lei's fair e-cash scheme are examined.

A. Initialing

Initially, the bank publishes a one-way hash function H and its public key $n(=p_1p_2)$, where p_1 and p_2 are large primes and $p_1 \equiv p_2 \equiv 3(\text{mod } 4)$. Similarly, the judge also publishes a bit string ω and its public key $\hat{n}(=p_3p_4)$, p_3 and p_4 are large primes, $p_3 \equiv p_4 \equiv 3(\text{mod } 4)$, and $\hat{n} = p_3p_4 > n$.

This research is supported in part by the National Science Council of the Republic of China under grant NSC89-2213-E002-167.

P.-L. Yu is currently a Ph.D. candidate in the Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106, R.O.C. (Tel: +886-2-23635251 ext.361. e-mail: bey@fractal.ee.ntu.edu.tw).

C.-L. Lei is with the Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106, R.O.C. (Tel: +886-2-23635251 ext.361. e-mail: lei@cc.ee.ntu.edu.tw).

B. Acquiring a tuple from the judge

In this phase, a customer acquires some tuples from the judge in order to withdraw e-cash sometime later. The major purpose of this phase is to let the judge choose b , u and v for the customer, so that the judge are able to revoke the anonymity on future illegal activities. After receiving the customer's request, the judge reacts as the following:

1. The judge randomly selects u, v, z, b in Z_n^* and computes $\hat{z} = (H(z))^{1/2}$. z is used as an unique identifier of this instance and \hat{z} is the signature of z .
2. The judge sends the tuple (b, u, v, \hat{z}, z) to the customer via secure manner and stores the tuple (u, v, b, z) in its database.

C. Withdraw

After acquiring a valid tuple from the judge, the customer can withdraw a coin from the bank with the tuple at any time. The withdraw protocol is as follows:

1. The customer randomly selects m and computes $\alpha = H(m)(u^2 + v^2) \bmod n$. Then he sends the tuple (α, z, \hat{z}) to the bank.
2. The bank randomly choose an integer δ and computes $x = H(\delta)$ such that $(\alpha(x^2 + 1) \bmod n)$ is a QR in Z_n^* . The bank then sends (x, z, \hat{z}) to the judge.
3. The judge retrieves (u, v, b, z) from its database and computes $c = ((ux + v)(u - vx)^{-1} \bmod n)$. If c does not collide with previous instances, the judge computes $\lambda = (b^2(u - vx) \bmod n)$. Then the judge records (u, v, b, z, c) in its another database and sends λ to the bank.
4. The bank computes $e = (\lambda^{-1} \bmod n)$ and derives an integer t in Z_n^* such that $t^4 \equiv \alpha(x^2 + 1)e^2 \pmod{n}$. The bank stores the tuple (δ, z) in its database and sends (t, e) to the customer.
5. The customer computes $s = bt \bmod n$ and $c = b^2e(ux + v) \bmod n$ and verifies the validity of the coin (m, c, s) by examine if $s^4 \equiv H(m)(c^2 + 1) \pmod{n}$.

D. Paying

In order to pay the money to the shop, the customer sends the coin (m, c, s) to the shop. After verifying $s^4 \equiv H(m)(c^2 + 1) \pmod{n}$, the shop deposits the coin (m, c, s) to the bank for on-line double-spending check. If the coin is fresh, the bank adds the corresponding amount to the shop's account.

E. Analysis

This scheme exposes a few serial drawbacks. First, the judge has to take a heavy computational burden because it has to participate in each tuple acquiring and coin withdrawing. Second, the judge has to record several items for each acquired tuple or withdrawn coin, so it must maintain huge databases. Finally, the judge may become a bottleneck because it has to on-line participate in each withdrawing.

III. THE PROPOSED SCHEME

In our proposed scheme, the customer has to apply an anonymous certificate from the judge firstly in order to withdraw e-cash later. Then the customer can withdraw coins with this certificate. The details of each phase of the proposed scheme are presented in the following subsections.

A. Initializing

The initializing phase of our scheme is the same as that of [3] mentioned in section 2. The bank publishes its public key $n (= p_1 p_2)$ and an one-way hash function H . The judge also publishes its public key $\hat{n} (= p_3 p_4)$ and a bit string w . Besides, the judge also selects a secret binary string ζ .

B. Applying anonymous certificate

Whenever a customer intends to apply an anonymous certificate, the following steps take place:

1. After mutually authentication, the customer sends a request to the judge to acquire an anonymous certificate.
2. The judge randomly selects a bit string σ and an integer r , where r is both in Z_n^* and $Z_{\hat{n}}^*$. Next, the judge forms an anonymous ID token $I = (w || ID_{Customer} || \sigma)^2 \bmod \hat{n}$, where $ID_{Customer}$ represents the customer's identity. Then the judge seals the ID token by computing $I' = H(I)r^8 \bmod n$ and $r' = (r \oplus \zeta)^2 \bmod \hat{n}$.
3. The judge sends $(S_{judge}(I', r'), I, r^{-1})$ to the customer via secure channel. $S_{judge}(I', r')$ means judge's digital signature on (I', r') and is treated as an anonymous certificate.

The customer can request several anonymous certificates at a time or apply new certificates later on. Each anonymous certificate is unique, because the judge selects a random number σ for each certificate.

C. Withdrawing

With a valid anonymous certificate, the customer can withdraw e-cash at any time. The withdrawing protocol is as follows:

1. The customer choose three random integers m, u , and v in Z_n^* such that $\alpha = H(m)(u^2 + v^2) \bmod n$ is in Z_n^* . He then sends α and $S_{judge}(I', r')$ to the bank.
2. The bank randomly selects x in Z_n^* such that $(I'(\alpha(x^2 + 1))^3 \bmod n)$ is a QR in Z_n^* and sends x to the customer.
3. The customer randomly selects a integer $b \in Z_n^*$, and computes $\delta = b^4 \bmod n$ and $\beta = \delta(u - vx) \bmod n$. He then submits β to the bank. The random number b is considered as the blinding factor.
4. The bank firstly computes $\lambda = (\beta^{-1} \bmod n)$, then derives an integer $t \in Z_n^*$ satisfying $t^8 \equiv_n I'(\alpha(x^2 + 1))^3 \lambda^6$. It sends (t, λ) to the customer.
5. The customer computes $s = b^3 r^{-1} t \bmod n$ and $c = \delta \lambda (ux + v) \bmod n$ to remove the blinding factor b . Finally, the customer verifies if the coin (I, m, s, c) satisfies $s^8 \equiv_n H(I)(H(m)(c^2 + 1))^3$.

D. Paying

In order to pay the money to the shop, the customer sends the coin (I, m, c, s) to the shop. The shop firstly checks whether the ID token I appears in the blacklist published by the judge. Then the shop verifies $s^8 \equiv_n H(I)(H(m)(c^2 + 1))^3$. If everything passes, the shop deposits the coin (I, m, c, s) to the bank for on-line double-spending check. If the coin is fresh, the bank adds the corresponding amount to the shop's account.

E. Coin tracing

In our scheme, the bank can send the anonymous certificate, say (I', r') , supplied by the suspicious customer to the judge. After receiving (I', r') , the judge computes $r = (r'^{\frac{1}{8}} \bmod \hat{n}) \oplus \zeta$ and $H(I) = I' r^{-8}$. Meanwhile, the judge adds $H(I)$ into the blacklist and informs all shops not to accept the coins including $H(I)$.

F. Owner tracing

In our framework, each coin contains an anonymous ID token issued by the judge. When we want to recover the linkage of one coin, say (I, m, s, c) , we only have to send the tuple to the judge together with enough evidence. Then the judge derives the square roots of I , and picks

the one prefixed with ω , i.e. $(\omega || ID_{Customer} || \sigma)^2 = I \bmod \hat{n}$. $ID_{Customer}$ is exactly the person who withdraw the coin.

IV. ANALYSIS

In this section, we prove that the fundamental fair blind signature scheme proposed in this paper is correct. Additionally, we analyze the properties of our scheme and compare it with [3].

A. Correctness

Proposition 1. *If (I, m, s, c) is a valid coin produced by our e-cash system, then*

$$s^8 \equiv_n H(I)(H(m)(c^2 + 1))^3.$$

Proof. Since both $(I'(\alpha(x^2 + 1))^3)$ and λ^6 are QR's in Z_n^* , there exists t in Z_n^* such that

$$\begin{aligned} t^8 &\equiv_n I'(\alpha(x^2 + 1))^3 \lambda^6. \text{ Thus,} \\ s^8 &\equiv_n (b^3 r^{-1} t)^8 \\ &\equiv_n b^{24} \cdot r^{-8} \cdot (I'(\alpha(x^2 + 1))^3 \lambda^6) \\ &\equiv_n b^{24} \cdot r^{-8} \cdot r^8 H(I) \cdot (H(m)(u^2 + v^2)(x^2 + 1))^3 (b^4(u - vx))^{-6} \\ &\equiv_n H(I) \cdot (H(m)(u^2 + v^2)(x^2 + 1)(u - vx)^{-2})^3 \\ &\equiv_n H(I) \cdot (H(m)((ux + v)^2 + (u - vx)^2)(u - vx)^{-2})^3 \\ &\equiv_n H(I) \cdot (H(m)((ux + v)(u - vx)^{-1} + 1))^3 \\ &\equiv_n H(I) \cdot (H(m)((b^4(ux + v) \cdot b^{-4}(u - vx)^{-1} + 1))^3 \\ &\equiv_n H(I) \cdot (H(m)((\delta(ux + v)\lambda)^2 + 1))^3 \\ &\equiv_n H(I) \cdot (H(m)(c^2 + 1))^3. \blacksquare \end{aligned}$$

B. Properties

In this subsection, we will briefly discuss various properties of our proposed scheme. Formal proofs of the claims will be given in the full paper and will be omitted here due to room limitation.

Unlinkability Because of the blinding factor b , the bank cannot link the withdrawn cash (I, m, s, c) with the data items (α, I', r', β) appeared in withdrawing phase. As a result, the anonymity property is guaranteed as long as the customer acts normally.

Unforgability To forge an e-cash coin (I, m, s, c) , a faker could choose (m, s, c) firstly and then derive the 8th root of $H(I) \cdot (H(m)(c^2 + 1))^3$. However, it is computationally infeasible to compute modular square root without knowledge of factors of n . In the other way, a faker could determine s at first and then derive corresponding (m, s, c) . It is also infeasible because H is an one-way hash function.

Randomization In the proposed withdraw protocol, the bank can choose x to randomize the being-signed message. Consequently, our scheme achieves randomization property.

Fairness In the proposed scheme, we adopt anonymous certificates to approach fairness property. As long as a customer behaves legally, his privacy will be well protected because no one can link up I and I' except the judge. However, the linkage can be recovered with the judge's help if illegal activities are detected. Coin tracing and owner tracing mechanisms are described in the section 3.

C. Performance

The computational performance of the proposed withdraw protocol is similar to [3], so user-efficient property still remains. The total communication overhead is reduced slightly since the bank need not consult with the judge during withdraw phase anymore.

On the other hand, the judge's storage requirement is totally freed in our scheme. The judge does not need to record anything for issued anonymous certificates. In addition, the judge's computational overhead could be reduced, because an anonymous certificate can be used to withdraw as many coins as the customer wants. However, the coins withdrawn with the same certificate could be linked together, so the amount of coins a certificate can be used to withdraw had better be limited. The worst case is just to withdraw each coin with a different anonymous certificate.

Moreover, the proposed scheme does not need on-line trusted third party. In our scheme, the judge is only involved when customers want to apply anonymous certificates. In fact, a customer can apply anonymous certificates beforehand.

V. CONCLUSION

In this paper, we have proposed a new approach to achieve fairness property based on Fan and Lei's scheme[3]. In our scheme, the judge is only involved in anonymous certificate signing. Each anonymous certificate can be reused for many coin withdrawing. Additionally, since anonymous certificates could be applied at any time before withdrawing, the judge will not forms a bottleneck. Furthermore, the judge need not store anything. As a result, our scheme is more efficient and practical.

REFERENCES

- [1] S. Brands, "Untraceable off-line cash in wallets with observers," *Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Science*, 773, Springer-Verlag, pp. 302-318, 1993.
- [2] D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," *Advances in Cryptology - Proceedings of Crypto'88*, pp. 319-327.
- [3] C. I. Fan and C. L. Lei, "A User Efficient Fair Blind Signature Scheme for Untraceable Electronic Cash," *Journal of Information Science and Engineering*, accepted, 2000. (A preliminary version of the paper appeared in *Proceedings of National Computer Symposium 1997*, Vol. 2, pp. C-89-C-94, 1997.)
- [4] C. I. Fan, and C. L. Lei, "User Efficient Blind Signatures," *IEEE Electronics Letters*, Vol. 34, No. 6, pp. 544-546, 1998.
- [5] Y. Frankel, Y. Tsiounis, and M. Yung, "Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-cash," *Advances in Cryptology-Asiacrypt'96, Lecture Notes in Computer Science*, 1163, Springer-Verlag, pp. 286-300, 1996.
- [6] M. Jakobsson, D. M'Raihi, and M. Yung, "Electronic Payments: Where Do We Go from Here?" *CQRE'99, Lecture Notes in Computer Science*, 1740, Springer-Verlag, pp. 43-63, 1999.
- [7] A. Juels, "Trustee Tokens : Simple and Practical Anonymous Digital Coin Tracing," *FC'99, Lecture Notes in Computer Science*, 1648, Springer-Verlag, pp. 29-45, 1999.
- [8] H. Peterson and G. Poupard, "Efficient Scalable Fair Cash With Off-line Extortion Prevention," *ICICS'97, Lecture Notes in Computer Science*, 1334, Springer-Verlag, pp. 463-477, 1997.
- [9] M. Stadler, J. M. Piveteau, and J. Camenisch, "Fair Blind Signature," *Advances in Cryptology-EUROCRYPT'95, Lecture Notes in Computer Science*, 921, Springer-Verlag, pp.209-219, 1995.
- [10] S. von Solms and D. Naccache, "On Blind Signatures and Perfect Crime," *Computer & Security*, 11, pp. 581-583, 1992.
- [11] J. Traore, "Making Unfair a 'Fair' Blind Signature Scheme," *ICICS'97, Lecture Notes in Computer Science*, 1334, Springer-Verlag, pp.386-397, 1997.



AbstractPlus

BROWSE

SEARCH

IEEE XPLORE GUIDE

SUPPORT

[View Search Results](#) | [Previous Article](#) | [Next Article](#)
[e-mail](#) [printer friend](#)

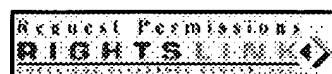
Access this document

Full Text: PDF (320 KB)

Download this citation

Choose Download » [Learn More](#)

Rights & Permissions

» [Learn More](#)

An user efficient fair e-cash scheme with anonymous certificates

Pei-Ling Yu Chin-Laung Lei

Dept. of Electr. Eng., Nat. Taiwan Inst. of Technol., Taipei, Taiwan;

This paper appears in: **Electrical and Electronic Technology, 2001. TENCON. Proceedings of IEEE Region 10 International Conference on**

Publication Date: 19-22 Aug. 2001

Volume: 1

On page(s): 74 - 77 vol.1

Number of Pages: 2 vol.(xviii+xvi+917)

Meeting Date: 08/19/2001 - 08/22/2001

INSPEC Accession Number: 7174603

Digital Object Identifier: 10.1109/TENCON.2001.949554

Posted online: 2002-08-07 00:30:23.0

Abstract

E-cash is considered as one of the coming mainstreams of digital currency due to its excellent security properties. With its perfect anonymity, however, e-cash may be misused to commit crimes. We propose a fair e-cash scheme, which improves previous schemes by reducing the computational and storage overhead of the trusted third party. In addition, our proposed scheme also possesses the desired user efficient property where a customer only has to compute a few modular multiplications and additions in coin withdrawal. Due to the rapidly growing Internet access via mobile units with low computation power, this user efficient property is of great worth. Thus this work can provide an efficient and practical payment mechanism for electronic commerce

Index Terms

Inspec

Controlled Indexing

[Internet](#) [certification](#) [electronic money](#) [mobile computing](#) [security of data](#)

Non-controlled Indexing

[Internet access](#) [addition](#) [anonymous certificates](#) [coin withdrawal](#) [computational overhead](#) [digital currency](#) [electronic commerce](#) [mobile units](#) [multiplication](#) [network security](#) [payment mechanism](#) [perfect anonymity](#) [security properties](#) [storage overhead](#) [trusted third party](#) [user efficient fair e-cash scheme](#) [user efficient property](#)

Author Keywords

Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEE Xplore.

[View Search Results](#) | [Previous Article](#) | [Next Article](#)




AbstractPlus

[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)[SUPPORT](#)
[View Search Results](#) | [Previous Article](#) | [Next Article](#)
[e-mail](#) [printer friendly](#)

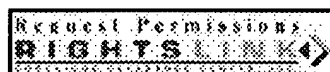
Access this document

Full Text: PDF (208 KB)

Download this citation

Choose [Citation](#)Download [EndNote, ProCite, RefMan](#)» [Learn More](#)

Rights & Permissions

» [Learn More](#)

Distributed electronic payment system based on bank union

[Qiang Xu](#) [Hong Zhao](#)

Software Center, Northeastern Univ., Shenyang, China;

This paper appears in: **High Performance Computing in the Asia-Pacific Region, 2000. Proceedings. The Fourth International Conference/Exhibition on**

Publication Date: 14-17 May 2000

Volume: 1

On page(s): 548 - 551 vol.1

Number of Pages: 2 vol. xxiv+1179

Meeting Date: 05/14/2000 - 05/17/2000

Location: Beijing

INSPEC Accession Number: 6590501

Digital Object Identifier: 10.1109/HPC.2000.846614

Posted online: 2002-08-06 23:18:23.0

Abstract

With the development of e-commerce, electronic payment systems based on the Web have become a research hotspot. Most current payment models are based on the single bank, and e-cash has a lack of transparency and interoperation generally. Therefore, we put forward a distributed electronic payment system model based on bank union. It adopts a two-level secure architecture to guarantee the security of the payment system and to realize the e-cash's transparency and interoperation. Moreover, on the base of it, we design a distributed payment gateway, and verify the security and performance of the system after its implementation.

Index Terms

Inspec

Controlled Indexing

[EFTS](#) [Internet](#) [bank data processing](#) [electronic money](#) [information resources](#) [security of data](#) [software performance evaluation](#)

Non-controlled Indexing

[World Wide Web](#) [bank union](#) [data security](#) [distributed electronic payment system](#) [distributed payment gateway](#) [electronic commerce](#) [interoperation](#) [performance](#) [two-level secure architecture](#)

Author Keywords

Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEE Xplore.

[View Search Results](#) | [Previous Article](#) | [Next Article](#)

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.c](#)

© Copyright 2005 IEEE - All Rights Reserved

Distributed Electronic Payment System Based on Bank Union *

Qiang Xu Hong Zhao

(Software Center of Northeastern University, Shenyang, P.R.C)

xuq@neu.edu.cn zhaoh@neu.edu.cn

Abstract

With the development of E-Commerce, Electronic Payment System based on Web has become the researching hotspot. But most of current payment models are based on the single bank, and e-cash is lack of transparency and interoperation generally. Therefore, this paper brings forward a distributed electronic payment system model based on bank union. It adopts a two-level secure architecture to guarantee the security of the payment system and to realize the e-cash's transparency and interoperation. Moreover, on the base of it, we design a distributed payment gateway, and verify the security and performance of the system after its implementation.

1. Introduction

Internet, the only media that can connect the whole world, has become a locale which has unlimited commerce. Electronic Payment System (EPS) has obvious advantages over the traditional, paper-based transactions, not only in terms of cutting-off costs in manufacturing, shipping and managing the physical material, but also in terms of speeding up the circulation of money. Therefore, EPSs will become the new direction of the Internet E-Commerce. But currently the EPSs are developed by commercial banks independently, and each bank should setup its own payment gateways and authenticating centers. So it will lead to the orderless competition and resource wasting, and the operation of every bank is

limited in a small range^[1]. Therefore, to guarantee the e-cash's security, transparency and interoperation, this paper brings forward a distributed electronic payment protocol model based on bank union, designs and implements a distributed EPS gateway based on it.

2. Architecture of distributed electronic payment system

Bank Union is a large group of banks, monitored by the Central Bank, where each bank can dispense e-cash. The payment protocol based on Bank Union should have the following properties:

- 1.No bank should be able to trace any e-cash it issues.
- 2.There is a single public key for the entire Bank Union.
The size of this public key is independent of the number of banks. Moreover, the public key should not be modified if more banks join the union.
- 3.Given a valid piece of e-cash only the Central Bank can tell which bank in the union issued it.
- 4.Neither the Central Bank nor any bank can issue e-cash on behalf of another bank.

According to these, we design a distributed EPS architecture, which has two-level secure structure, shown in figure 1. The VPN layer based on IP Security provides data origin authentication, data integrity, and replay protection by using AH, ESP and IKE^[2] to guarantee the security and integrity of the data and provide the communication level's authenticating service and tunnel for the distributed EPS. And the distributed payment

* Supported in part by 863 HTRDP under the contract 863-306-ZT05-05-5.

protocol based on Bank Union provides the security, transparency and interoperation of the application level's payment procedure by restrict blind signature^[3] and group blind signature^[4].

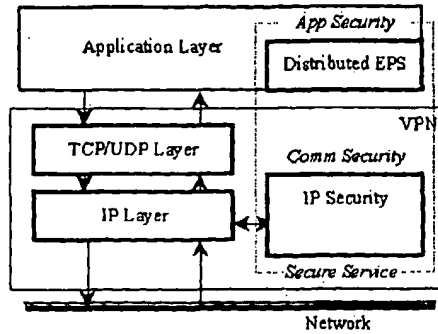


Figure 1. Architecture

3. Distributed electronic payment protocol

The distributed electronic payment protocol model is shown in figure 2.

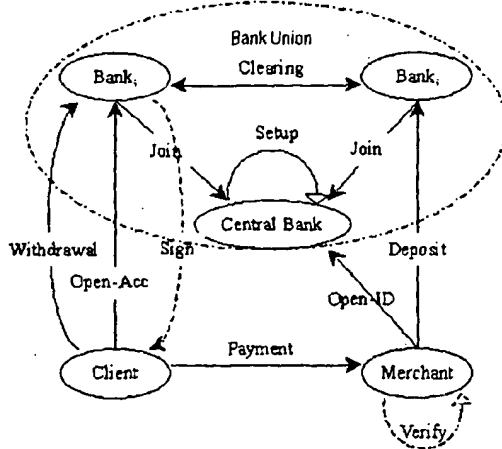


Figure 2. Protocol model

3.1 Protocol definition

Definition 1. Set an ideal hash function $H : \{0,1\}^* \rightarrow \{0,1\}^k$ satisfying the following properties:

1. For a specified parameter l , $H_l(x)$ is collision-resistant;
2. $H_0 : G_q \times G_q \times \text{Merchant} \times \text{ID} \times \text{DATE} / \text{TIME} \rightarrow Z_q$.

Definition 2. A signature of knowledge of a double

discrete logarithm of y to the base g and a , on message m , with security parameter $l \leq k$ denoted

$\text{SKLOGLOG}_l[\alpha|y = g^{(a^e)}](m)$, is an $(l+1)$ -tuple

$(c, s_1, \dots, s_l) \in \{0,1\}^k \times Z_n^l$ satisfying the equation

$$c = H_l(m, y, g, a, P_1, \dots, P_l), \text{ where } P_i = \begin{cases} g^{(a^i)}, & c[i] = 0 \\ y^{(a^i)}, & c[i] \neq 0 \end{cases}$$

Definition 3. A signature of knowledge of an e -th root of the discrete logarithm of y to the base g , on message m ,

denoted $\text{SKROOTLOG}_l[\alpha|y = g^{(a^e)}](m)$, is an $(l+1)$ -tuple

$(c, s_1, \dots, s_l) \in \{0,1\}^k \times Z_n^l$ satisfying the following equation:

$$c = H_l(m, y, g, e, P_1, \dots, P_l), \text{ where } P_i = \begin{cases} g^{(s_i^e)}, & c[i] = 0 \\ y^{(s_i^e)}, & c[i] \neq 0 \end{cases}$$

3.2 Bank union protocol

1. Union Setup Protocol—Setup

The Central Bank chooses a generator-tuple (g, g_1, g_2) , a security parameter l and computes the following values:

1. An RSA Public Key (n, e) , where $\text{length}(n) > 2l$ bits.
2. A cyclic group $G = \langle g \rangle$ of order n , where G is a cyclic subgroup of Z_p^* and p is a prime and $n \mid (p-1)$.
3. An element $\alpha \in Z_p^*$ where α has large multiplicative order modulo all the prime factors of n .
4. An upper bound λ on the length of the secret keys and a constant $\mu > 1$.

So the union's public key is $\Upsilon = (n, e, G, g, \alpha, \lambda, \mu)$.

2. Member Join Protocol—Join

In order to join the Bank Union, Bank_i should perform the join protocol shown in figure 3, where x is Bank_i's private key, y is one part of Bank_i's public key, and v is Bank_i's membership certificate.

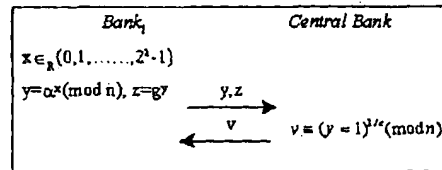


Figure 3. Join protocol

3.3 Commerce trading protocol

1. Signature Procedure—Sign

In order to sign the e-cash, $Bank_i$ does the following:

1. Obtain $q \in_R Z_n^*$ and set $\tilde{g} := g^q, \tilde{z} := g^{-q}$.
2. For $\forall 2^\lambda \leq u_i \leq 2^{\lambda+\mu} - 1 \wedge v_i \in_R Z_n^* (1 \leq i \leq l)$, set

$$P_i^{SKLOGLOG} := g^{-(u_i)}, P_i^{SKROOTLOG} := g^{-v_i}.$$

3. Send $(g, z, \{P_i^{SKLOGLOG}\}, \{P_i^{SKROOTLOG}\})$ to Client.

4. For $b \in_R \{1 \dots 2^\lambda - 1\} \wedge f \in_R Z_n^*$, sets $w := (af)^*(\text{mod } n)$,

$$\hat{g} := g^{-w}, \hat{z} := z^{-w}, \hat{P}_i^{SKLOGLOG} := (P_i^{SKLOGLOG})^w,$$

$$\hat{P}_i^{SKROOTLOG} := (P_i^{SKROOTLOG})^w \text{ and compute:}$$

$$V_1 = SKLOGLOG_1[\alpha | \hat{z} = \hat{g}^{\alpha}] (e\text{-cash})$$

$$V_2 = SKROOTLOG_1[\beta | \hat{z} \hat{g} = \hat{g}^{\beta}] (e\text{-cash})$$

The resulting signature on e-cash consists of

$(\hat{g}, \hat{z}, V_1, V_2)$ and can be verified by checking correctness of V_1 and V_2 .

2. Tracing Protocol—Open-ID

Given a signature $(\hat{g}, \hat{z}, V_1, V_2)$ for an e-cash, the Central Bank can determine the signer by testing if

$\hat{g}^{\hat{z}} = \hat{z}$ for each union member $Bank_i$ (where $y_{Bank_i} = \log_g z_{Bank_i}$ and z_{Bank_i} is $Bank_i$'s membership key).

The Central Bank can establish the identity of the signer without giving away y_{Bank_i} using the signer's membership key z_{Bank_i} , the signer's commitment to

z_{Bank_i} , and a non-interactive proof that $\log_g z = \log_g \hat{z}$.

3. Open Account Protocol—Open-Acc

In order to open an account in $Bank_i$, Client should

perform the Open-Acc protocol shown in figure 4, where l is the only account identity in $Bank_i$ and zz is another part of $Bank_i$'s public key.

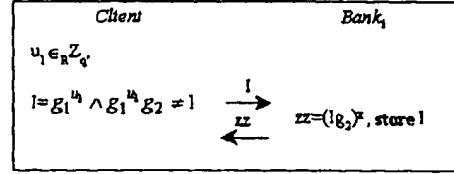


Figure 4. Open-Acc protocol

4. Withdrawal Protocol—Withdrawal

When Client wants to withdraw an e-cash, he firstly should prove ownership of his account and perform the following protocol shown in figure 5.

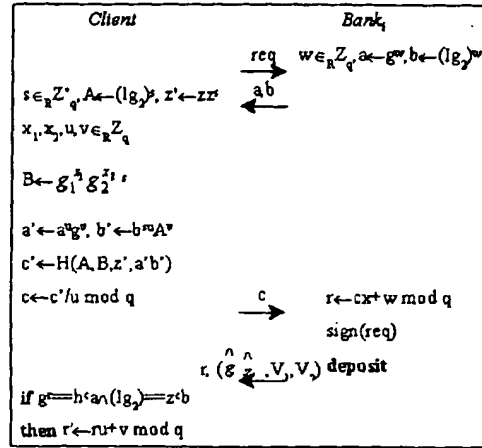


Figure 5. Withdrawal protocol

5. Payment Protocol—Payment

When Client wants to spend his e-cash at Merchant, the following protocol shown in figure 6 is performed.

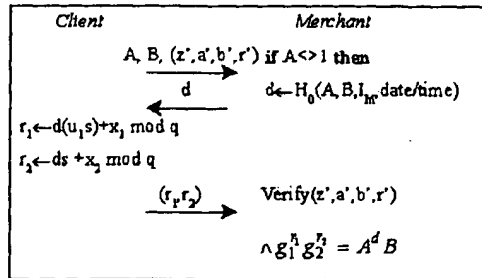


Figure 6. Payment protocol

6. Deposit Protocol—Deposit

After some delay in time, Merchant sends the payment transcript to $Bank_i$, consisting of A, B ,

$(z', a' b' r')$, (r_1, r_2) , $(\hat{g}, \hat{z}, V_1, V_2)$ and date/time of transaction.

If $A=1$, then $Bank_i$ does not accept the payment transcript. Otherwise, $Bank_i$ computes d using the supplied date/time of transaction. $Bank_i$ then verifies that

$$g_1^d g_2^z = A^d B \text{ and } (z', a' b' r') \text{ is a signature on } (A, B). \text{ If}$$

not both verifications hold, then $Bank_i$ does not accept the payment transcript. Otherwise, $Bank_i$ searches its deposit database to find out whether A has been stored before. There are two possibilities:

- A has not been stored before. In that case, $Bank_i$ stores $(A, \text{date/time}, r_1, r_2)$ in its deposit database as being deposited by Merchant, and credits the account of Merchant. If Merchant's account is $Bank_j$, the clearing procedure is needed to clear between $Bank_i$ and $Bank_j$'s deposit database.

- A has already in the deposit database. In that case, a fraud must have occurred. If the already stored transcript was deposited by Merchant and date/time are identical to that of the new payment transcript, then Merchant is trying to deposit the same transcript twice. Otherwise, the e-cash has been double-spent. Since $Bank_i$ now has at its disposal a pair (d, r_1, r_2) from the new transcript and a pair (\hat{d}, r_1', r_2') from the deposited information, it can

compute $g_1^{(\eta_1 - \hat{\eta}_1)/(\eta_2 - \hat{\eta}_2)}$. $Bank_i$ then searches its account database for this account number; the corresponding account-holder is the double-spender. The number $(\eta_1 - \hat{\eta}_1)/(\eta_2 - \hat{\eta}_2) \bmod q$ serves as a proof of double-spending; it is equal to $\log_{g_1} I$, with I the account number of the double-spender.

The security of this protocol is based on the assumptions that the discrete logarithm, double discrete logarithm, and the roots of discrete logarithm problems are hard. So it is exactly as secure as Camenisch's Basic Group Signature Scheme^[4].

4. System design and implementation

According to the above framework and technology,

we design and implement a VPN gateway, which has the ability of distributed electronic payment. It is based on the Intel/Linux platform, and is connected with Internet by synchronous network adapters.

It includes the following modules:

1. Transform and policy databases' maintaining module.
2. Incoming/outgoing packets' processing module.
3. Kernel interfaces module.
4. Management utilities.

Latency is the most important performance parameter. We measured latency using ping with different packet sizes and IPSec transforms. The result is shown in figure 7. Notice that the scale is logarithmic. The graph shows that the cost of authenticating does not really downgrade response time, but that encryption is a major bottleneck.

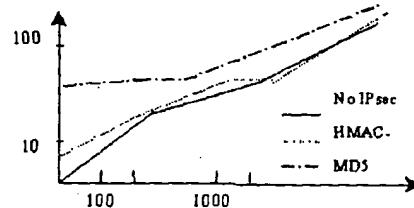


Figure 7. Ping performance

5. Conclusion

According to the current state of the EPS, we design and implement a distributed EPS based on Bank Union. It is running as a gateway, and is of high security and economy. So it gives a solution to current e-cash payment of Bank Union in some degree.

References

- [1] Asokan N.etc. The State of the Art in Electronic Payment Systems. IEEE Computer, Sep, 1997: 28-35.
- [2] Kent S. Security Architecture for the Internet Protocol. RFC2401, BBN, November 1998.
- [3] Brands S. Untraceable Off-line Cash in Wallets with Observers. In Proc. CRYPTO'93, Springer, 1994: 302-318.
- [4] Anna L., and Zulfikar R. Group Blind Signatures: A Scalable Solution to Electronic Cash. In Proc. Financial CRYPTO'98, Lecture Notes in Computer Science Vol.1455, pp184-197.